

page 1

DNSSEC: For a more secure Domain Name system

Forum on ccTLD for Policy makers, Regulators and Operators
Mauritius, 17-19 march 2009
aalain@afnic.net

page 2

Why DNSSEC

- Good security is multi-layered
 - Multiple defense 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

page 3

The Problem

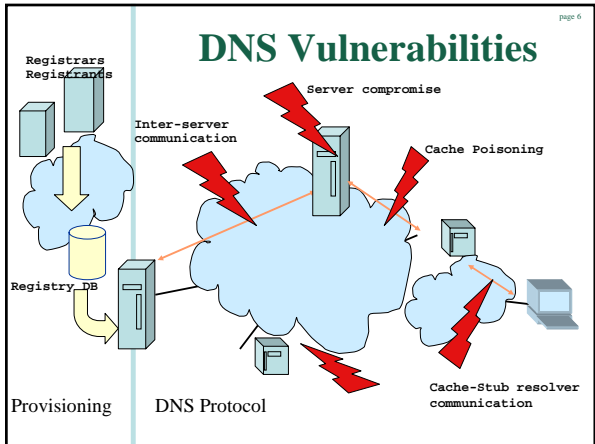
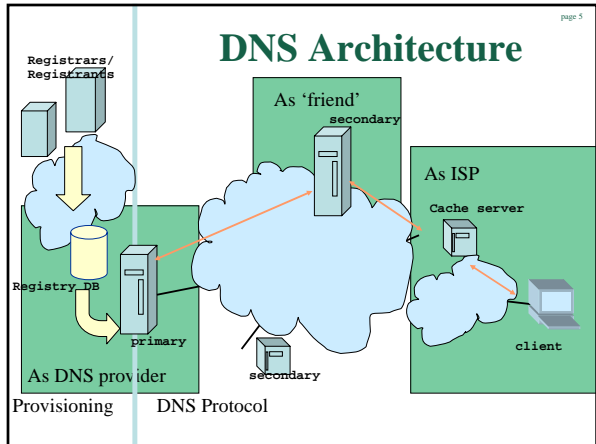
- DNS data published by the registry is being replaced on its path between the “server” and the “client”.
- This can happen in multiple places in the DNS architecture
 - DNS uses UDP, much easier to spoof
 - Some places are more vulnerable to attacks than others
 - Vulnerabilities in DNS software make attacks easier (and there will always be software vulnerabilities)
- Deficiencies in the DNS protocol and in common deployment create some weaknesses
 - Query ID is 16 bits (0-65535)
 - Lack of UDP packet Source Port (16 bits) and Query ID randomization in some deployments

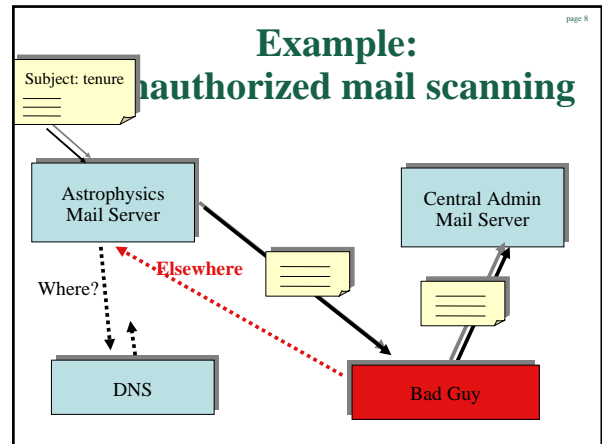
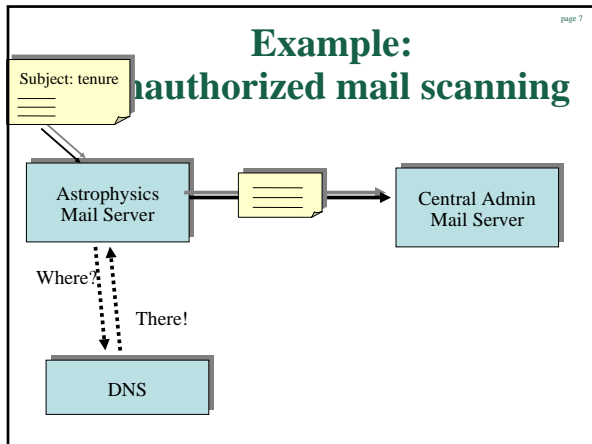
page 4

The Problem(cont'd)

- Kaminsky Attacks published in 07/2008 showed how these weaknesses can be exploited for cache poisoning attacks
 - Panic (although all of this is known for a long !!!)
 - Workarounds to contain the situation
 - Source port/Query ID randomization
 - Recommendations for DNS deployment
<http://www.kb.cert.org/vuls/id/800113>
 - The Solution ????
 - **DNSSEC**

And so, DNSSEC is now known as a critical component of DNS Security





page 9

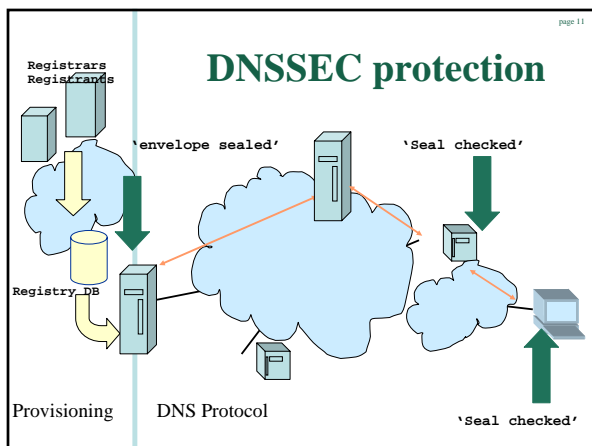
Where Does DNSSEC Come In?

- DNSSEC secures the name to address mapping
 - Transport and Application security are just other layers.

page 10

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



page 12

DNSSEC hypersummary

- Data authenticity and integrity by signing the Resource Records Sets with private key
- Public DNSKEYs used to verify the RRSIGs
- Children sign their zones with their private key
 - Authenticity of that key established by signature/checksum by the parent (DS)
- Ideal case: one public DNSKEY distributed

A signed zone

page 13

```
[...]
trstech.net. 86400 NS      ns.trstech.net.
trstech.net. 86400 NS      rip.psg.com.
trstech.net. 86400 RRSIG   NS 5 2 86400 20061227191027 (20061127191027 33888
trstech.net.pVuzETr5b3RjBR86HTDgrJVEkL9QH0uRoR3mepL5wGih8IeJpeZQNJQPZMAMzcEiDmli2RkXvpYlXtDtdBpdg
==)
[...]
trstech.net. 86400 DNSKEY 257 3 5 (
AwEAAZwNwvGbmAT+yW9K+XlK6WqN3FTheksfUUCjAVWLKyhK8B5+2GdCC7QW4MA3dwAKbpqv+4NSgByLwQzB
nF6gSRW3PnuR53u8F3yuzTo69HSL04okZfmXAWnDSJLJYOWkZyycB+IMWUWqEYWMmC5aZuTL7kHJndz3
; key id = 36472
[...]
trstech.net. 86400 RRSIG   DNSKEY 5 2 86400 20061227191027 (20061127191027 33888 trstech.net.
J82BTIEZOoheOMgh52SLtHXHj9jT12RlepZr9+EAeW/24wJqkicWLRN1DFYXtK1V24F9NzkU85TfFw==)
[...]
trstech.net. 3600 NSEC     aalain.trstech.net. NS SOA MX RRSIG NSEC DNSKEY
trstech.net. 3600 RRSIG   NSEC 5 2 3600 20061227191027 (20061127191027 33888 trstech.net.
TE9+FGO2Yf5fwOus3uXyW/Ub4M6YobJNkhTWW835F7zqmZprFLp5ZNAK200M901uY7X120O8mRDv8XXb9Q==)
[...]
```

Authenticity and Integrity

page 14

- We want to check authenticity and integrity of DNS data
- Authenticity: Is the data published by the entity we think is authoritative?
- Integrity: Is the data received the same as what was published?
- Public Key cryptography helps to answer these questions
 - use signatures to check both integrity and authenticity of data
 - Verify the authenticity of signatures

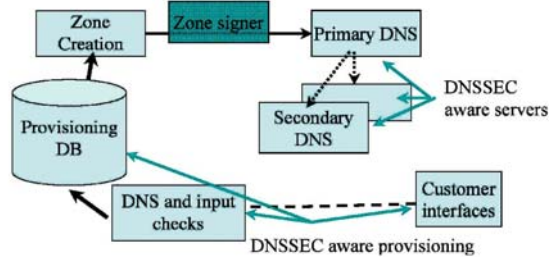
DNSSEC Deployment Tasks

page 15

- Key maintenance policies and tools
 - Private key use and protection
 - Public key distribution
- Zone signing and integration into the provisioning chain
- DNS server infrastructure
- Secure delegation registry changes
 - Interfacing with customers

DNSSEC Architecture modification

page 16



Using the DNS to Distribute Keys

page 17

- Secured islands make key distribution problematic
- Distributing keys through DNS:
 - Use one trusted key to establish authenticity of other keys
 - Building chains of trust from the root down
 - Parents need to sign the keys of their children
- Only the root key needed in ideal world
 - Parents always delegate security to child
 - ... but it doesn't help to sign if your parent doesn't sign, or isn't signed itself...

What do we do Until The Root Is Signed ?

page 18

- Use of Trust Anchors
 - A DNS resource record store that contains SEP (Secure Entry Point) keys for one or more zones.
- Two initiatives exist to provide these Trust Anchor Repositories.
 - for TLDs
 - for other domains

Trust Anchor Repositories... DLV and ITAR

page 19

DLV: DNSSEC Lookaside Validation

- Alternative method for chain of trust creation and verification in a disjointed signed space (islands of trust)
- DLV functions automatically (if the resolver is configured to do so) by looking up in a preconfigured “lookaside validation” zone
 - no need to fetch a list of anchors
 - ISC Initiative: <https://www.isc.org/solutions/dlv>

Trust Anchor Repositories... DLV and ITAR

page 20

ITAR: Interim Trust Anchor Repositories

- Interim Trust Anchor Repository
- IANA Trust Anchor Repository (Until The Root Is Signed)
 - Is targeted at TLDs
 - Lookup is not automatic
 - list of anchors must be retrieved (one more operational constraint)
 - Already a beta program, several TLDs have already registered
 - <https://itar.iana.org/>

TLDs and DNSSEC

page 21

- .bg (Bulgaria)
- .br (Brazil)
- .pr (Puerto Rico)
- .museum
- .se (Sweden)
- .cz (Czech Republic)
- .gov (is close)
- .org (is close)
- Several IDN-based TLDs
 - <https://itar.iana.org/>

Other DNS security

page 22

- We talked about data protection
 - The sealed envelope technology
 - RRSIG, DNSKEY, NSEC and DS RRs
- There is also a transport security component
 - Useful for bilateral communication between machines
 - TSIG or SIG0

Questions?

page 23

