DNSSEC and ENUM

Olaf M. Kolkman

olaf@nlnetlabs.nl

DNSSEC evangelist of the day

- NLnetLabs
  - Not for profit Open Source Software lab
    - Developed NSD
  - DNS and DNSSEC research
    - Protocol and software development
    - Deployment engineering
- Active IETF participant
  - co-chair of the IETF DNSEXT working group
  - member of the Internet Architecture Board
  - RFC 3757 and RFC 4061

Outline

- purpose and protocol
- Current Developments/problem areas
  - And the case for hand waving for ENUM
- Deployment

Bourtange, source Wikipedia

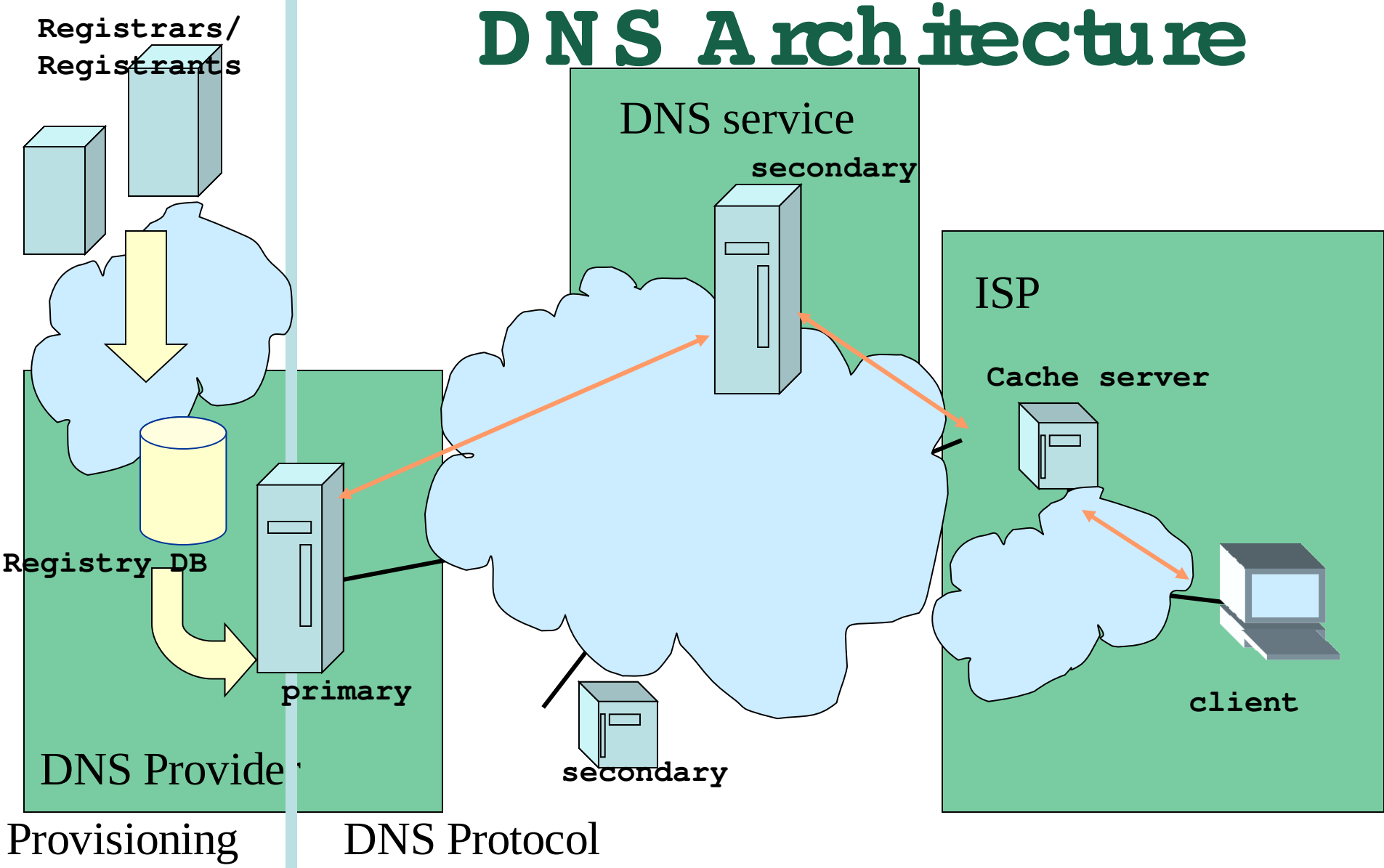
Why DNSSEC

- Defense layers
  - 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

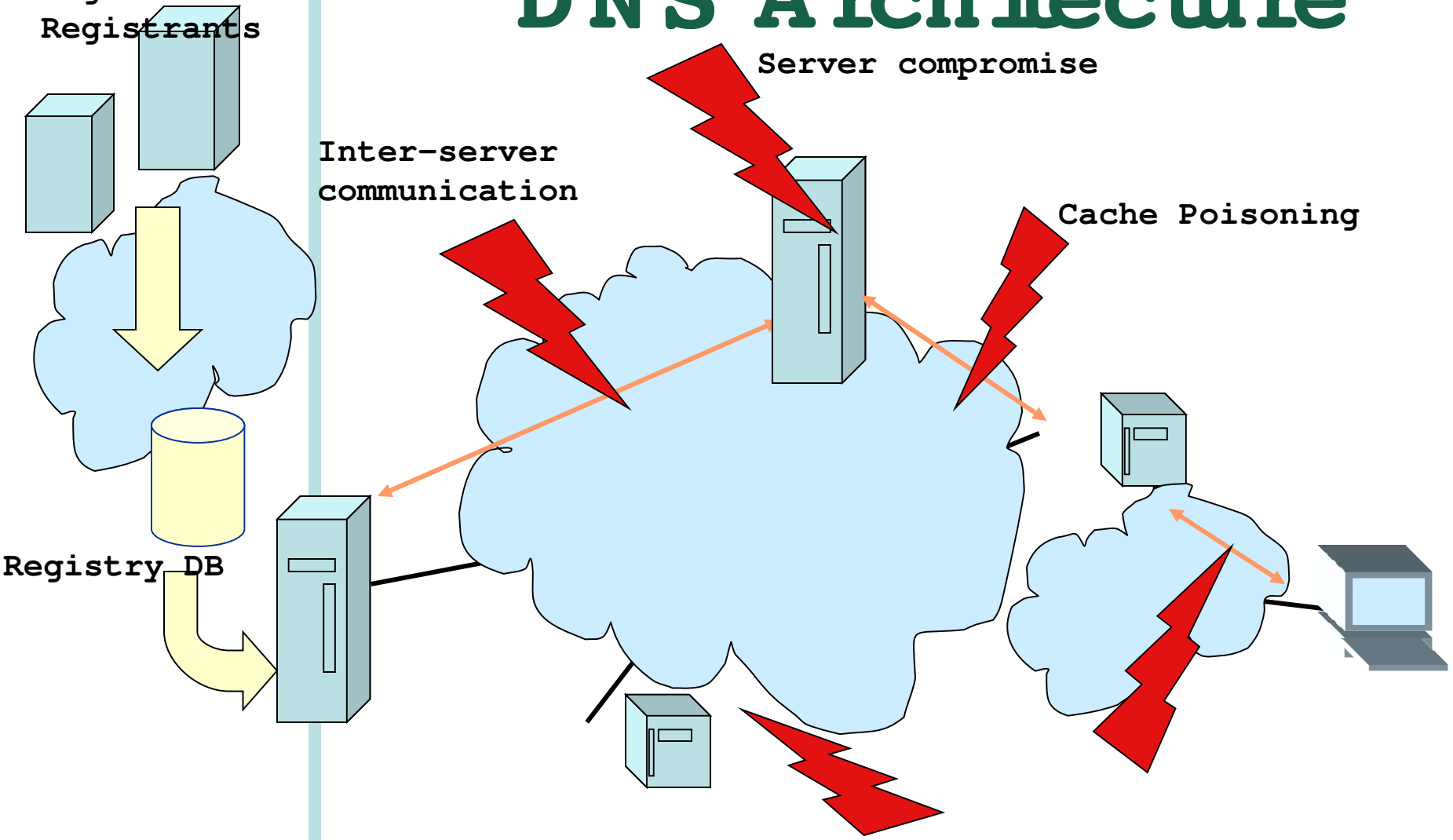
The Problem

- 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
  - Some places are more vulnerable to attacks then others
  - Vulnerabilities in DNS software make attacks easier
    (and there will always be software vulnerabilities)

DNS Architecture

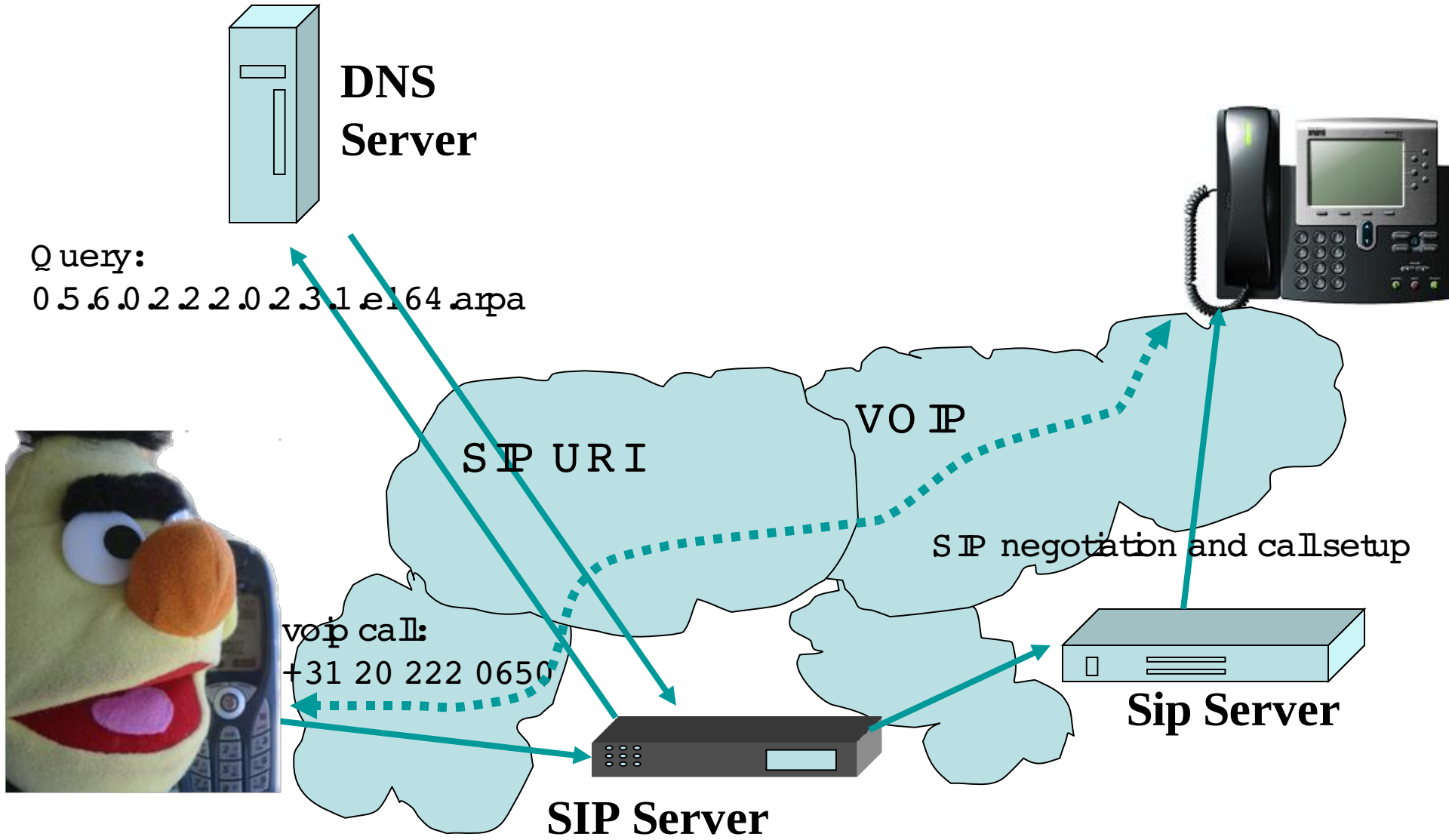


DNS Architecture

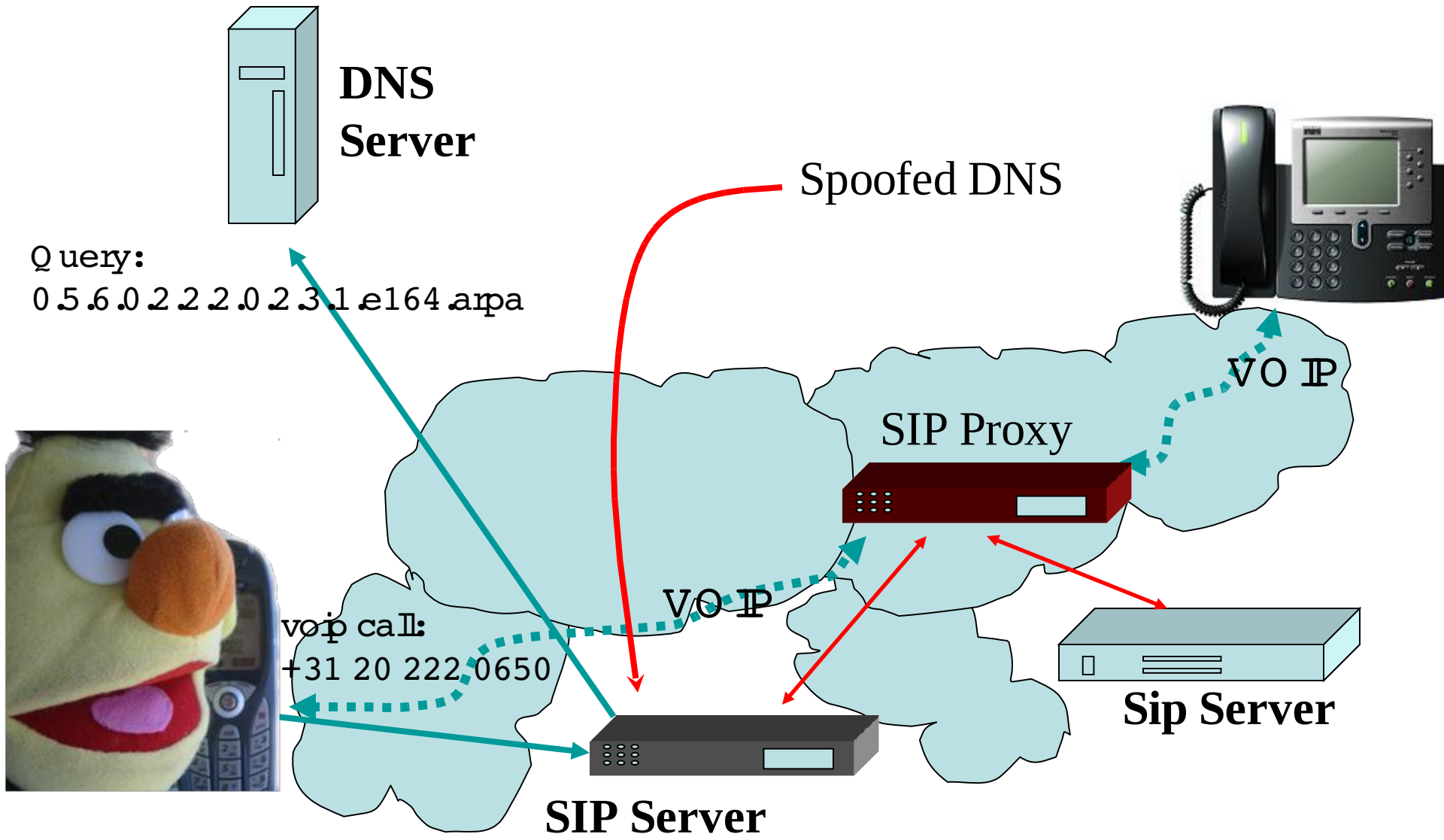


Provisioning DNS Protocol

voip2voip as an example



voip2voip as an example



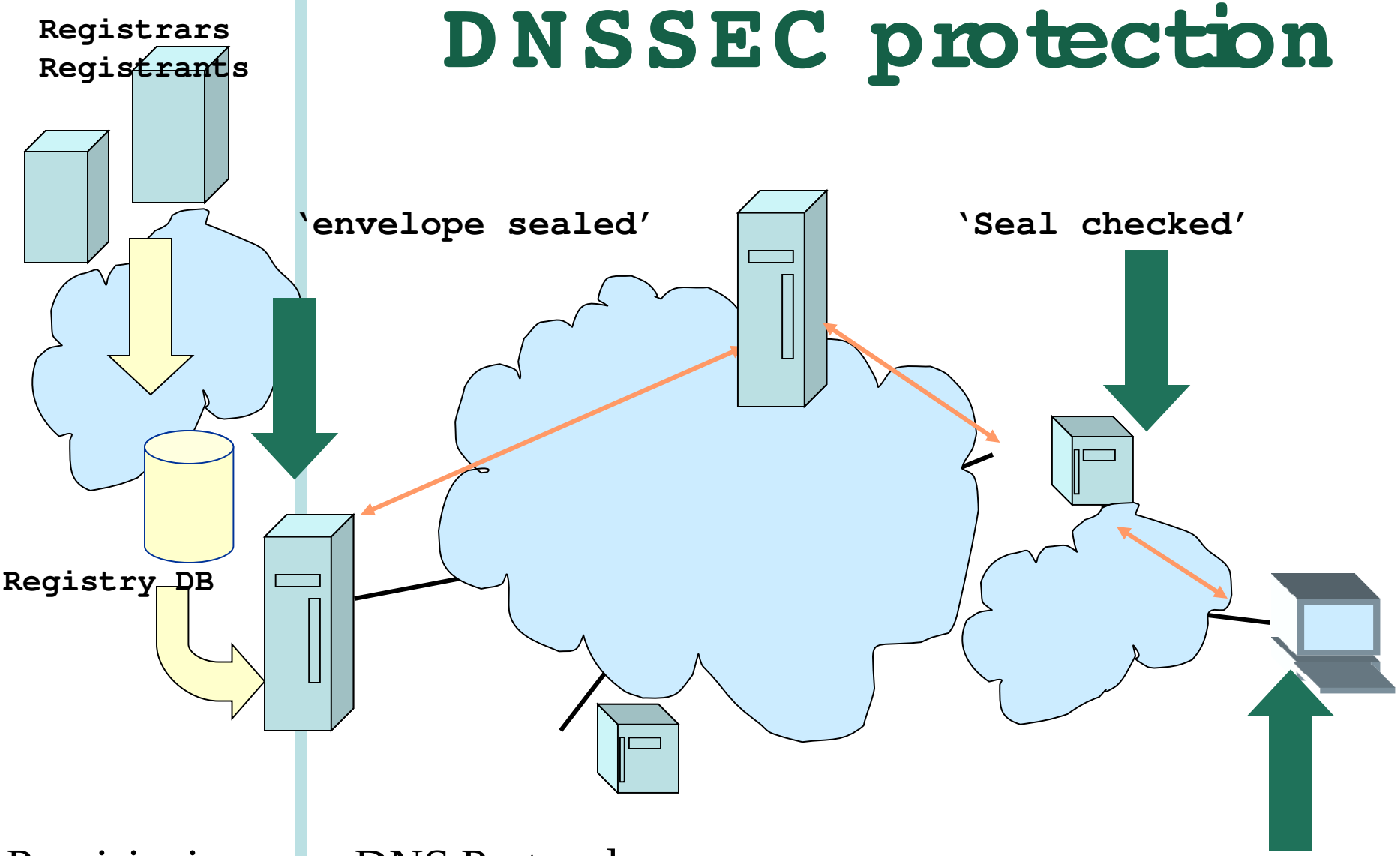
Where Does DNSSEC Come In?

- DNSSEC secures the name to resource record mapping
  - Transport and Application security are just other layers
- SIP itself allows for certificates
  - sip:olaf@goodsip.example
  - But ENUM obfuscates the URI:
    - x.x.x.1.3.e164.arpa → olaf@badsip.example
    - badsip.example certificate is cheap

Solution a Metaphor

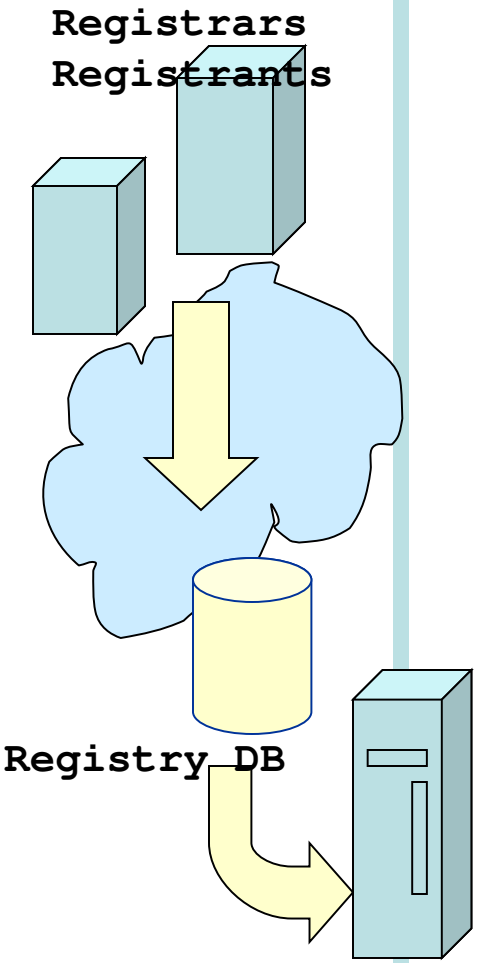
- Compare DNSSEC to a sealed transparent envelope.
- The seal is applied by whoever closes the envelope
- Anybody can read the message
- The seal is applied to the envelope, not to the message

DNSSEC protection



Provisioning DNS Protocol

DNSSE does not protect provisioning



Provisioning

www.zone-h.org - Seen a different Zone-H or Google.de?

SEEN A DIFFERENT ZONE-H OR GOOGLE.DE?

Written by SyS64738
Tuesday, 23 January 2007

Have you recently seen a different Zone-H when trying to access our pages? Magic of DNS redirection.

It appears that Saudi Arabia crackers managed to get the passwords of our registrar (our registrant panel to be precise), accessed the domain management page and changed the DNS entries, pointing the zone-h domain to an IP address belonging to the crackers on which they mounted the page you saw in the last 48 hours.

48 hours!?! So long it took to take contact with the registrar (they work only through email communication), explain the problem to 8 different people then finally getting a reset of our credentials, taking the domain back in control.

On the funny side, the same problem happened to Google in its German version which yesterday evening was redirected to a different page (different owner actually). **In this case** (automatic German/English translation) the trick was a bogus domain transfer request that a German provider accepted without explicit authorization from Google Inc. (silence-consense).

What a day! We are so glad we deserve so much of attention.

PS: you will soon find the mirrors in our DB as even though Zone-H wasn't hacked, from the users' point of view it appeared defaced, as only a few users realized they weren't visiting the actual Zone-H server. From the historycal point of view exactly the **same incident** happened to the Al jazeera sat tv network website, where a hacker managed to trick the registrar to send him the domain control passwords after sending a bogus passport copy during the ID verification process, subsequently changing Al Jazeera's DNS pointing to a different server.

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

DNSSEC secondary benefits

- DNSSEC provides an "independent" trustpath
  - The person administering "https" is most probably a different from person from the one that does "DNSSEC"
  - The chains of trust are most probably different
  - See acm queue.org article: "Is Hierarchical Public-Key Certification the Next Target for Hackers?"

More 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"

DNSSEC is an enabling technology

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
- It does not provide protection against DDOS

Outline

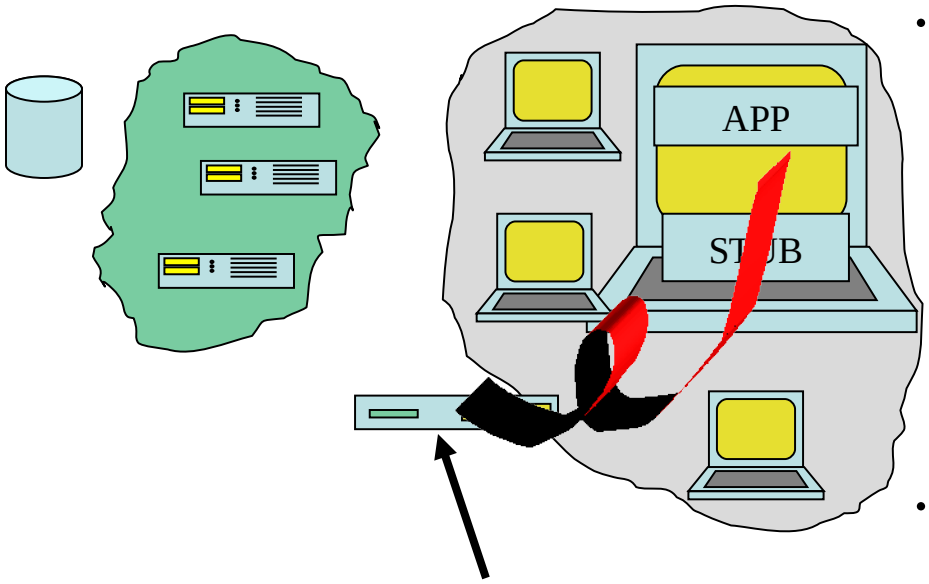
- purpose and protocol
- Current developments/problem areas
- Deployment

Main Problem Areas

improvement

- "the last mile"
- Key management and key distribution
- NSEC walk

The last mile

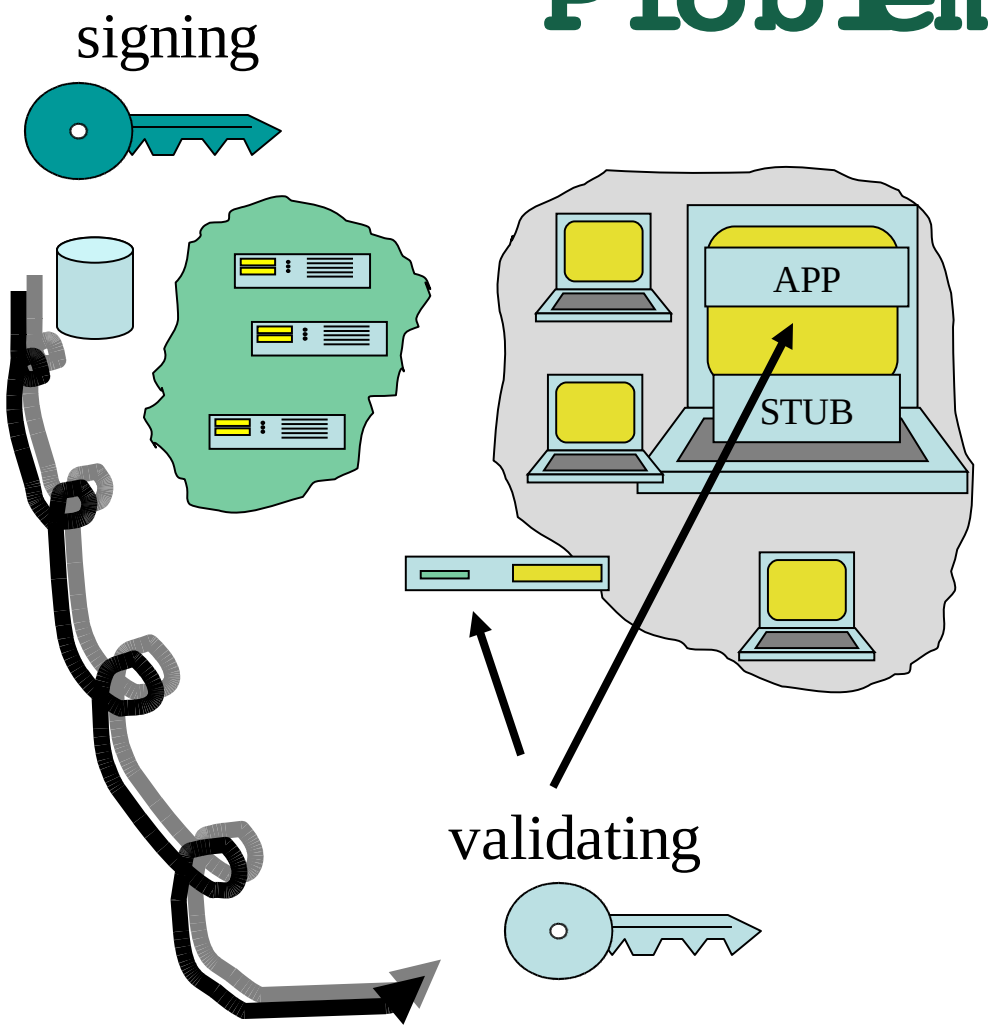


- How to get validation results back to the user
- The user may want to make different decisions based on the validation result
  - Not secured
  - Time out
  - Crypto failure
  - Query failure
- From the recursive resolver to the stub resolver to the Application

ForENUM

- ForENUM, trusted channel between SIP Server and the validating recursive name server.
  - Can be deployed today

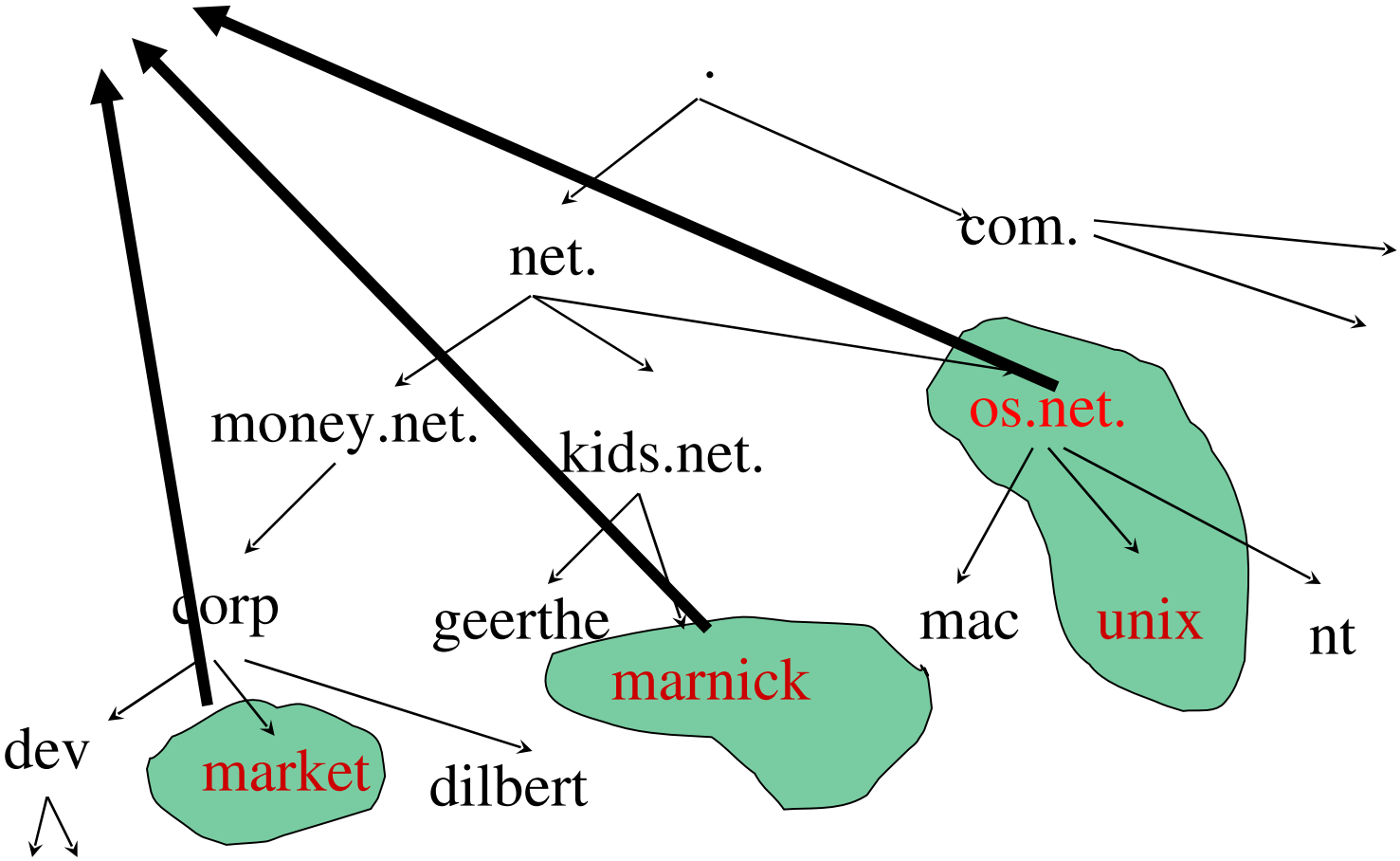
Problem Area



Key Management

- Keys need to propagate from the signer to the validating entity
- The validating entity will need to "trust" the key to "trust" the signature.
- Possibly many islands of security

Secure Islands and key management



For ENUM:

- e164.arpa needs to be signed
  - Probably sooner than the root
- Rollover still applies
  - Protocol to assist with rollover is in last stages of IETF process

NSEC walk

- The record for proving the non-existence of data allows for zone enumeration
- Providing privacy was **not** a requirement for DNSSEC
- Zone enumeration does provide a deployment barrier

But, for ENUM

- Walking is a non-issue (as it is trivial)
  - DNS properties allow to walk the tree efficiently
    - Technical detail: Difference between RCODEs
    - Easy to find out where the tree stops and where it has depth

Preventing NSEC walk Current Work

- Online creation and signing of NSEC RRs that cover the query name
  - RFC 4470 and RFC 4471
- NSEC3
  - Hashed based denial of existence
  - draft-ietf-dnsext-nsec3
    - Working group finished: IETF Last Call in a couple of weeks
    - Implementations exist.

Outline

- purpose and protocol
- Current Developments/problem areas
- Deployment

Common arguments against

- DNSSEC is to complex to deploy
  - The weapon with which to shoot oneself in the foot is not a pop-gun but a military grade full automatic
- The root will never get signed
- There is no economy to push deployment
- Cache poisoning can be mitigated by correctly implementing random query ports and proper query ID
- The specification is still a moving target

What's keeping folk

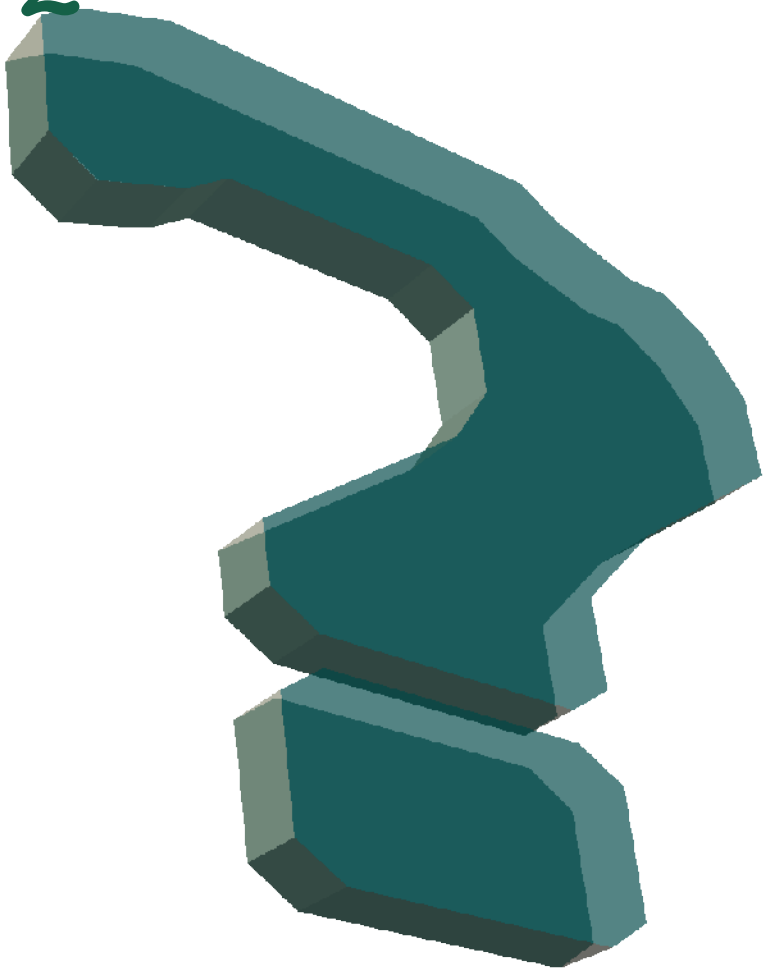
- New technology; chicken and egg
- Zone walking possibility
  - Is this really an issue in your environment?
- Automated key rollover and distribution

- Solutions for both are in the final stages of standardization

Concluding remarks

- DNSSEC is not a magic bullet but will become an important component
  - Through providing the DNSSEC infrastructure one enables apps and resolver to innovate.
- ENUM has a strong use case
  - Responsibility for the registries to provide protective means
- U.S. Federal requirement
  - Federal agencies will need to support DNSSEC
  - http://www.dnssec-deployment.org/news/FISMA.htm

QUESTIONS?



Acknowledgements: A number of these slides are based on earlier work at RIPE NCC.

References I

Without claims to completeness...

RFCs can be found at http://www.ietf.org/rfc/

Internet drafts are at
http://www.ietf.org/internet-drafts/

- DNSSEC bis:
  - RFC 4033, 4034, 4035
- Authenticated denial:
  - Online signing:
    - RFC 4470, RFC 4471
  - NSEC3: draft-ietf-dnsext-dnssec-nsec3

Rerferences II

Key Anchorm aintenance

- DLV: IEICE Trans. Commun. Vol. E88-B, No. 4, April 2005
- Trustanchorm aintenance (standards track):
  - draft-ietf-dnsext-trustupdate-threshold
- Old proposals:
  - draft-ietf-dnesxt-trustupdate-timers
  - draft-moreau-dnsext-takrem-dns
  - draft-laurie-dnssec-key-distribution

References III
Operational

- RFC 4641
- RIPE 352
  - http://www.ripe.net/ripe/docs/ripe-352.html
- DNSSEC HOWTO
  - http://www.nlnetlabs.nl/dnssec_howto/
- draft-hayatnagarkar-dnsext-validator-api
- Geoff Hustons experiences
  - ispcolumn.isoc.org or www.potaroo.net

References IV
Websites

- www.dnssec-deployment.org
- www.dnssec.net
- RIPE DNSSEC deployment (key management tools etc)
  - www.ripe.net/disi/
- DNSSEC testbed and testing tools developed by NIST
  - http://www-x.antd.nist.gov/dnssec/
- DNSSEC tools available at
  - http://www.dnssec-tools.org/

References V
Deployment Initiatives

- http://dnssec.nic.se/
- http://www.dnssec.ru/
- https://www.ripe.net/rs/reverse/dnssec/