

Jaap Akkerhuis

NLnet Labs

DNSSEC

Securing the DNS protocol

Summary

- Introduction
- DNS 101
- DNS Security Extension
- Questions

Introducing myself

- Networking since '82
- Currently at NLnet Labs
- Active in RIPE, IETF, ICANN
- Got involved in DNSSEC while at SIDN

NLnet Labs

- Research Engineering
- NSD name server for authoritative service
 - Do one thing well (and fast)
 - Root servers, TLD, etc.
- DNSSEC operational testing (with SIDN)
- DNSSEC validation tools

Purpose of naming

- Addresses are used to locate objects
- Names are easier to remember than numbers
- You would like to get to the address or other objects using a name
- **DNS provides a mapping from names to resources of several types**

DNS

- A lookup mechanism for translating objects into other objects
- A globally distributed, loosely coherent, scalable, reliable, dynamic database
- Comprised of three components
 - A “name space”
 - Servers making that name space available
 - Resolvers (clients) which query the servers about the name space

DNS Features: Global Distribution

- Data is maintained locally, but retrievable globally
 - No single computer has all DNS data
- DNS lookups can be performed by any device
- Remote DNS data is locally cachable to improve performance

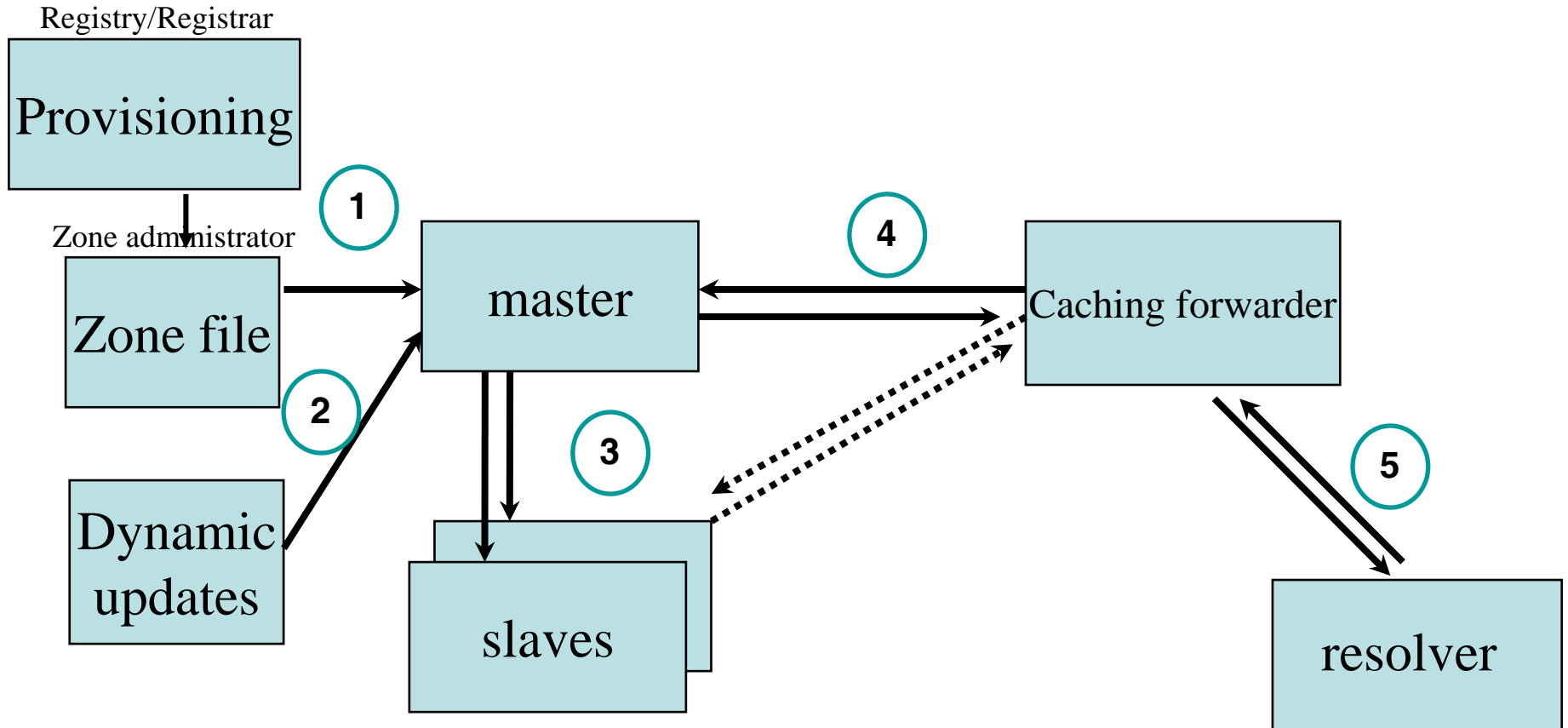
DNS Features: Scalability

- No limit to the size of the database
 - One server has over 90,000,000 names
 - Not a particularly good idea
- No limit to the number of queries
 - 24,000 queries per second handled easily
- Queries distributed among masters, slaves, and caches

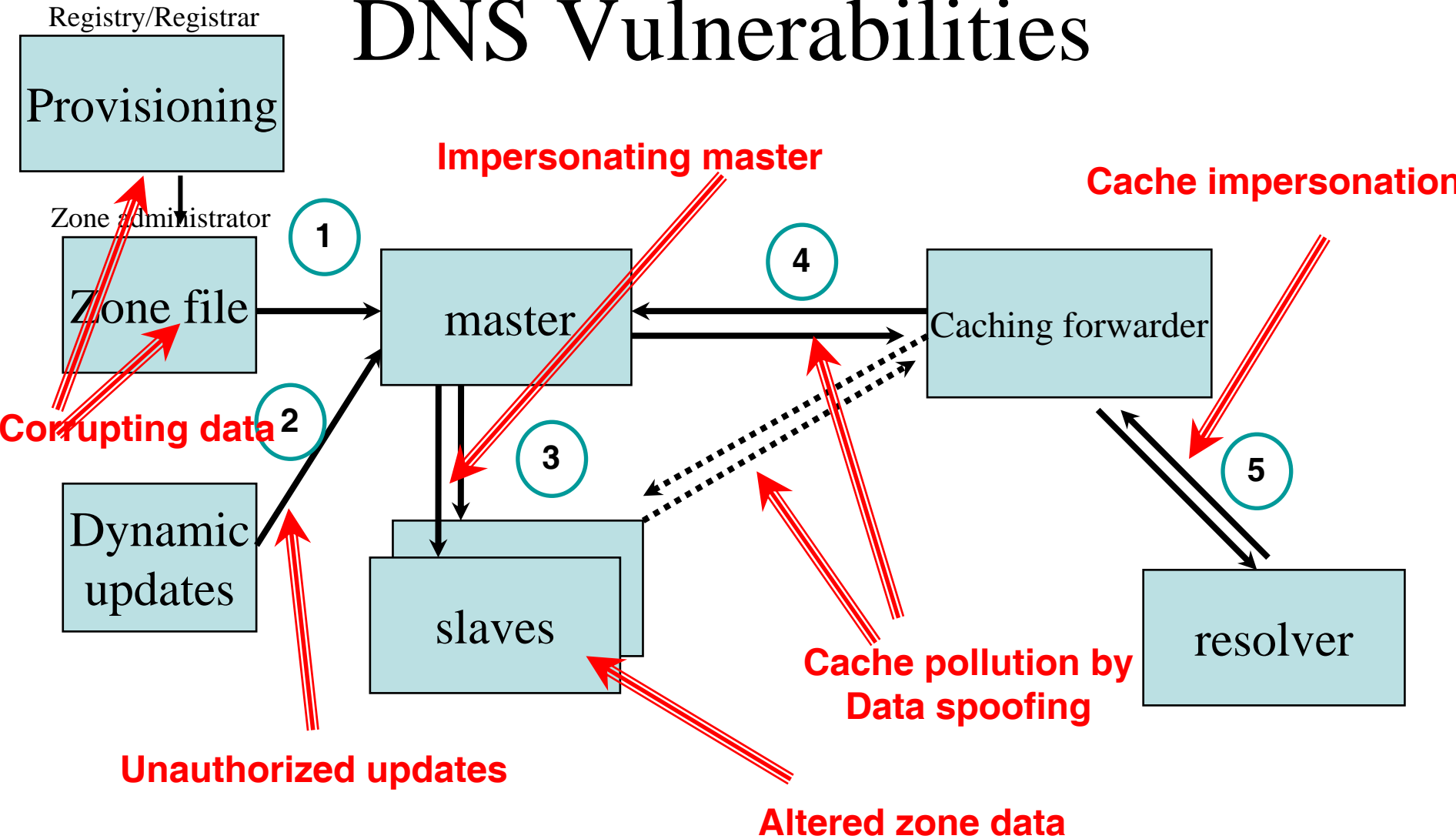
DNS Features: Reliability

- Data is replicated
 - Data from master is copied to multiple slaves
- Clients can query
 - Master server
 - Any of the copies at slave servers
- Clients will typically query local caches
- DNS protocols can use either UDP or TCP
 - If UDP, DNS protocol handles retransmission, sequencing, etc.

DNS: Data Flow

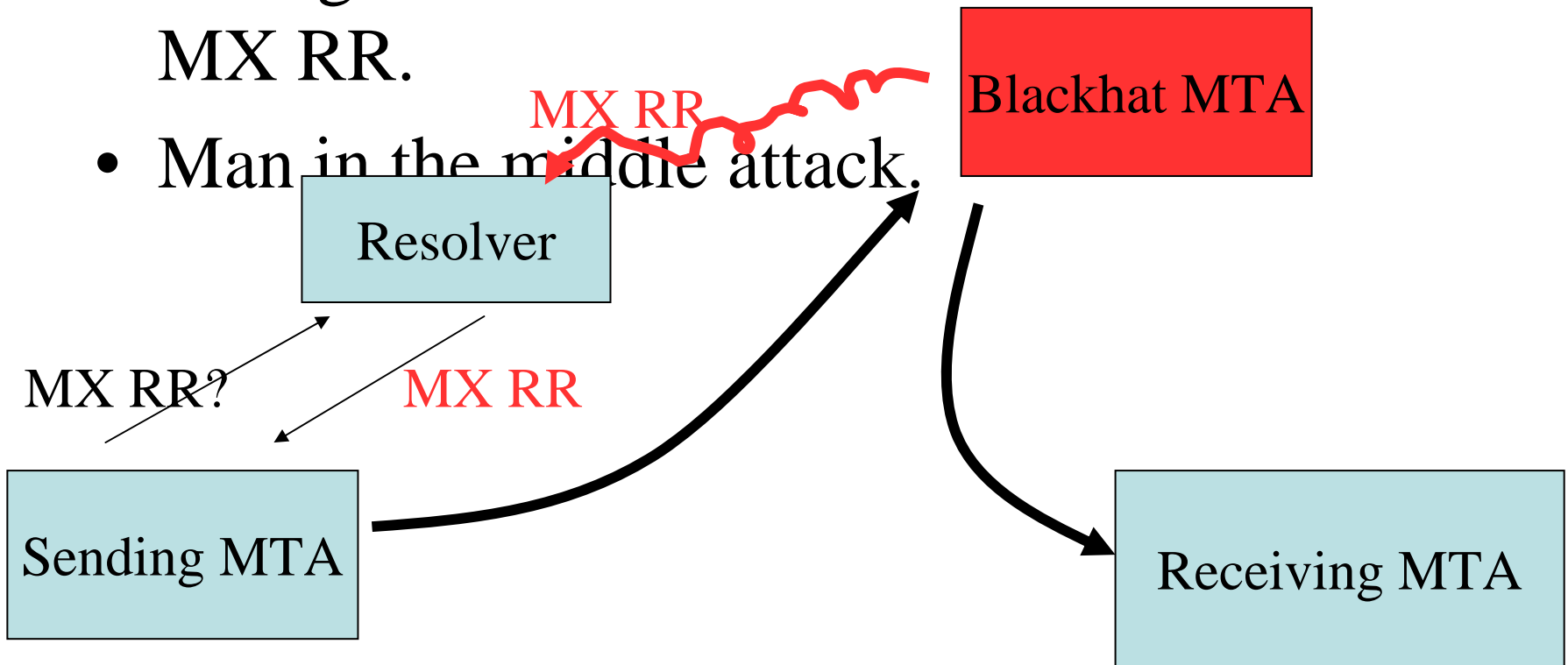


DNS Vulnerabilities



DNS exploit example

- Mail gets delivered to the MTA listed in the MX RR.
- Man in the middle attack.



Mail man in the middle

- ‘Ouch that mail contained stock sensitive information’
 - Who per default encrypts all their mails?
- We’ll notice when that happens, we have log files
 - You have to match address to MTA for each logline.

Other possible DNS targets

- SPF, DomainKey and family
 - Technologies that use the DNS to mitigate spam and phishing: \$\$\$ value for the black hats
- StockTickers, RSS feeds
 - Usually no source authentication but supplying false stock information via a stock ticker and via a news feed can have \$\$\$ value
- ENUM
 - Mapping telephone numbers to services in the DNS
 - As soon as there is some incentive

DNSSEC Characteristics

- Based on Public Private Encryption scheme
- Data is signed in the tree
- Public key available
- Authenticates the data
- Chain of trust

Mitigate by deploying SSL?

- Claim: SSL is not the magic bullet
 - (Neither is DNSSEC)
- Problem: Users are offered a choice
 - happens too often
 - users are not surprised but annoyed
- Not the technology but the implementation and use makes SSL vulnerable
- Examples follow

Example 1: mismatched CN

The image shows a Mozilla Firefox browser window with a security error dialog box and a certificate viewer window. The browser's address bar shows the URL <http://www.robcoadvies.nl/firsebrok>. The security error dialog, titled "Security Error: Domain Name Mismatch", contains the following text:

You have attempted to establish a connection with "www.robcoadvies.nl". However, the security certificate presented belongs to "www.robcodirect.nl". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.

If you suspect the certificate shown does not belong to "www.robcoadvies.nl", please cancel the connection and notify the site administrator.

Buttons: View Certificate, OK, Cancel, Help.

The certificate viewer window, titled "Certificate Viewer: 'www.robcodirect.nl'", shows the following details:

General | Details

This certificate has been verified for the following uses:
SSL Server Certificate

Issued To

Common Name (CN)	www.robcodirect.nl
Organization (O)	Robeco
Organizational Unit (OU)	Robeco Direct N.V.
Serial Number	6B:0B:F6:DB:74:C9:1E:1C:B6:52:9B:4E:82:43:EC:86

Issued By

Common Name (CN)	<Not Part Of Certificate>
Organization (O)	VeriSign Trust Network
Organizational Unit (OU)	VeriSign, Inc.

Validity

Issued On	6/18/2004
Expires On	6/19/2005

Fingerprints

SHA1 Fingerprint	39:A7:AB:1C:C3:64:FE:93:75:03:A3:4D:C5:DD:75:81:FE:12:98:46
MD5 Fingerprint	EE:21:4D:E3:B8:4A:EE:21:26:D0:4D:8C:CB:26:A7:87

Buttons: Help, Close.

Labels at the bottom of the image: www.robcoadvies.nl (with an arrow pointing to the "View Certificate" button) and www.robcodirect.nl (with an arrow pointing to the "Common Name (CN)" field in the certificate viewer).

Example 2: Unknown CA

Web Site Certified by an Unknown Authority

Unable to verify the identity of bert.secret-wg.org as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be bert.secret-wg.org, possibly leaking confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate and be willing to to accept this certificate for the purpose of identifying the web site bert.secret-wg.org?

Examine Certificate...

Accept this certificate permanently

Accept this certificate temporarily for this session

Do not accept this certificate and do not connect to this web site

OK **Cancel**

Certificate Viewer: "bert.secret-wg.org"

General Details

Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	bert.secret-wg.org
Organization (O)	Secret Working Group
Organizational Unit (OU)	Bert's Secretariat
Serial Number	01

Issued By

Common Name (CN)	Secret WG Certificate Authority
Organization (O)	Berts Root Certificate Authority
Organizational Unit (OU)	<Not Part Of Certificate>

Validity

Issued On	12/10/2004
Expires On	12/10/2005

Fingerprints


SHA1 Fingerprint	1F:DC:EC:50:B1:69:DB:74:3B:67:AD:1C:6C:DA:92:FA:9A:5A:1F:8D
MD5 Fingerprint	D5:E9:C1:11:1E:89:F8:A9:DE:57:F0:BC:7D:24:AD:5E

Help **Close**

Unknown Certificate Authority

Confused?

Security Alert



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

Web Site Certified by an Unknown Authority

Unable to verify the identity of bert.secret-wg.org as a trusted site.

Possible reasons for this error:


- Your browser does not recognize the site's certificate authority.
- The site's certificate is incomplete.
- You are connected to a site that is not intended to exchange confidential information.

Please notify the site's webmaster if you believe this is a problem.

Before accepting this certificate, you should be willing to accept this certificate from an unknown authority.


[Examine Certificate...](#)

Warning - Security




Do you want to accept the certificate from web site "www.p3.postbank.nl" for the purpose of exchanging encrypted information?

Publisher authenticity verified by: "VeriSign, Inc."



The security certificate was issued by a company that is not trusted.



The security certificate has not expired and is still valid.

Caution: "www.p3.postbank.nl" is not a trusted publisher. Do not accept this content if you trust your privacy.

[Yes](#)

company you have to determine whether

matching the name

Certificate

Security Alert



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.



The security certificate was not chosen to trust. View the certificate to determine if you want to trust the certificate.



The security certificate date is valid.



The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

[Yes](#) [No](#) [View Certificate](#)

Certificate signer not found

The server's certificate chain is incomplete, and the signer(s) are not registered. Accept?

bert.secret-wg.org [View](#)

- The certificate for "bert.secret-wg.org" is signed by the unknown Certificate Authority "Secret WG Certificate Authority". It is not possible to verify that this is a valid certificate

[Accept](#) [Install](#) [Cancel](#) [Help](#)

How does DNSSEC come into this picture

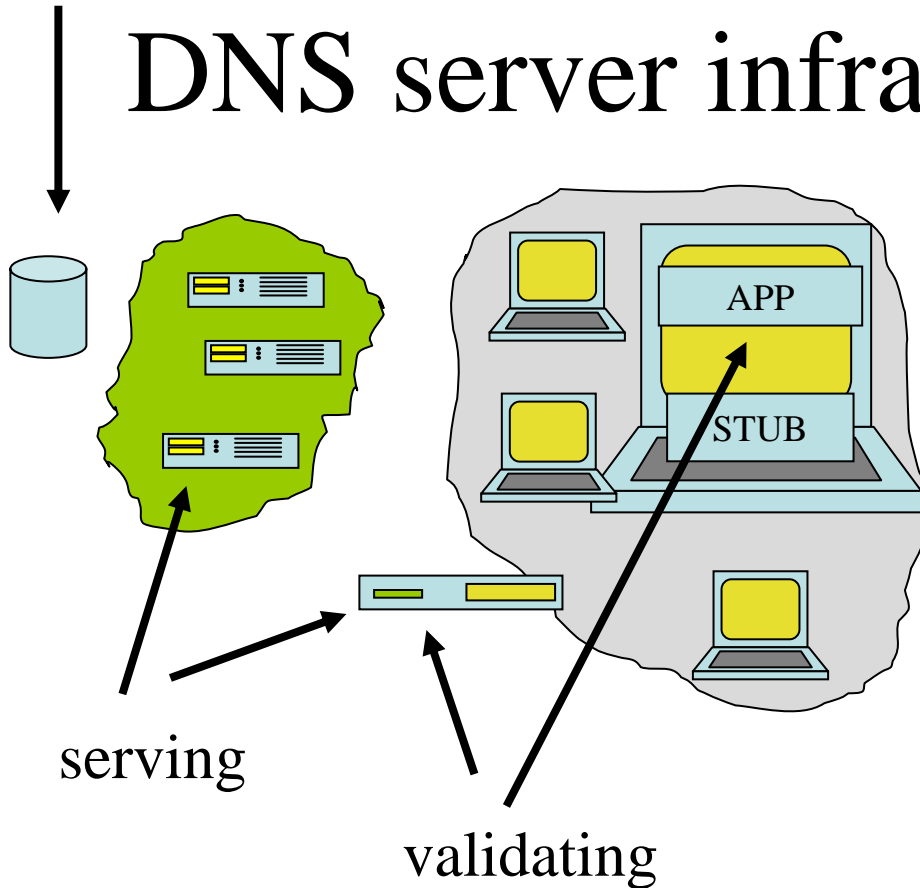
- DNSSEC secures the name to address mapping
 - before the certificates are needed
- DNSSEC provides an “independent” trust path.
 - The person administering “https” is most probably a different person from the one that does “DNSSEC”
 - The chains of trust are most probably different
 - See acmqueue.org article: “Is Hierarchical Public-Key Certification the Next Target for Hackers?”

Any Questions so far?

- We covered some of the possible motivations for DNSSEC deployment
- Next: What is the status of DNSSEC, can it be deployed today?

DEPLOYMENT NOW

DNS server infrastructure related



Protocol spec is clear on:

- Signing
- Serving
- Validating

Implemented in

- Signer
- Authoritative servers
- Security aware recursive name servers

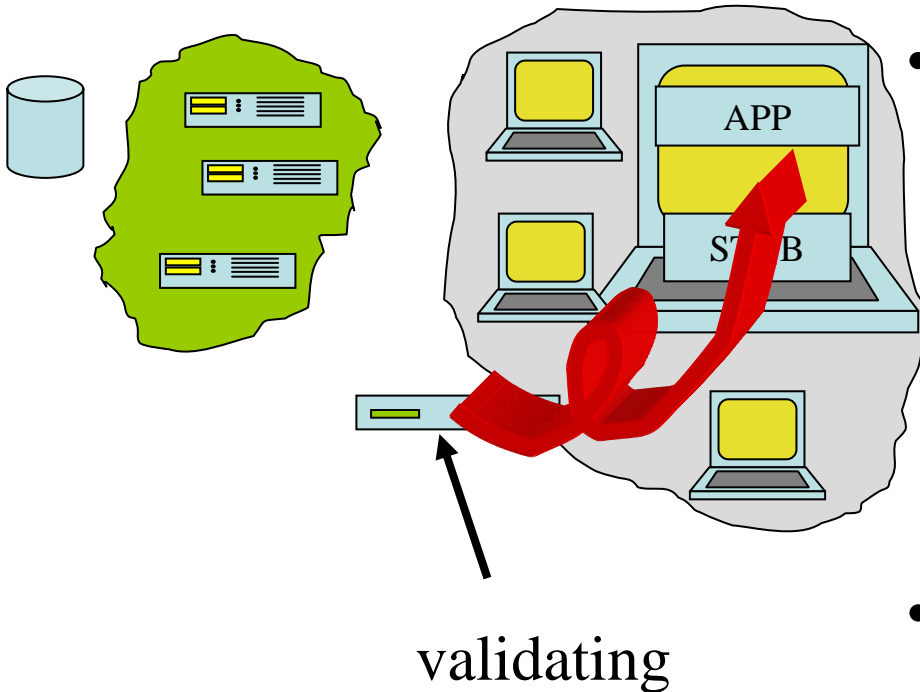
improvement

Main Problem Areas

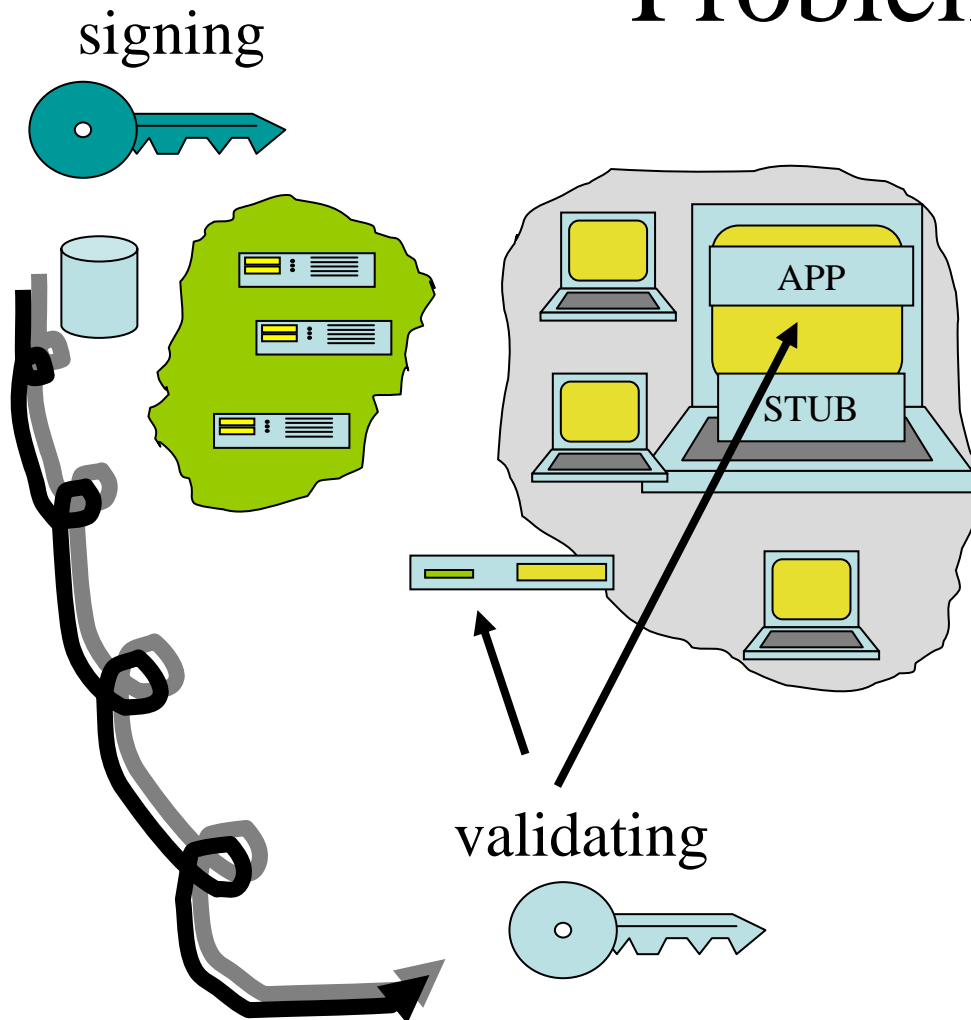
- “the last mile”
- Key management and key distribution
- NSEC walk

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



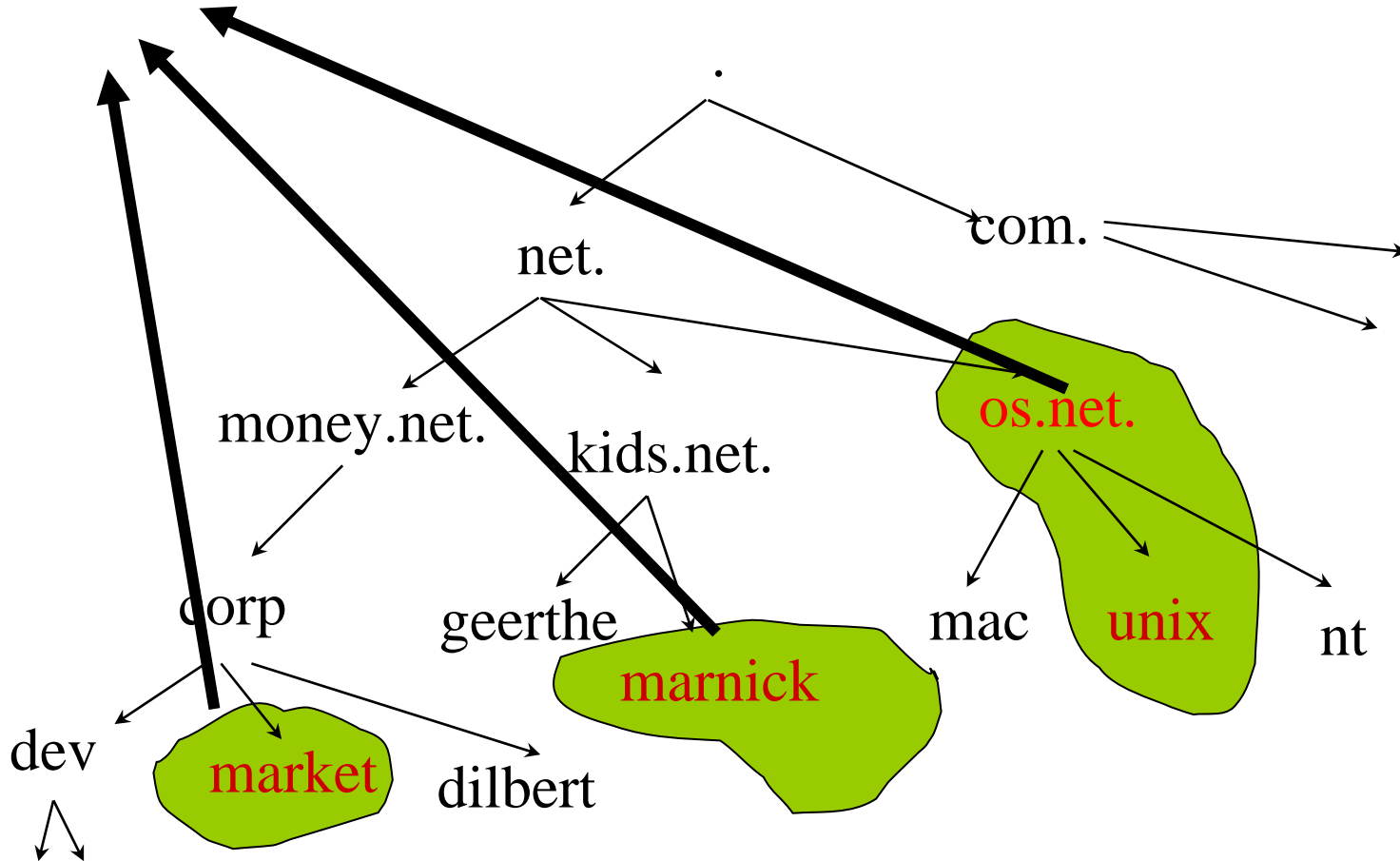
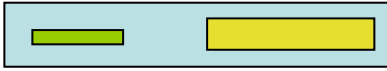
Problem Area



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



Secure Islands

- **Server Side**
 - Different key management policies for all these islands
 - Different rollover mechanisms and frequencies
- **Client Side**
(Clients with a few to 10, 100 or more trust-anchors)
 - How to keep the configured trust anchors in sync with the rollover
 - Bootstrapping the trust relation

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
- Work starting to study possible solutions
 - Requirements are gathered
 - If and when a solution is developed it will be co-existing with DNSSEC-BIS !!!
 - Until then on-line keys will do the trick.

Current work in the IETF

(a selection based on what fits on one slide)

Last Mile

- draft-gieben-resolver-application-interface

Key Rollover

- draft-ietf-dnsext-dnssec-trustupdate-timers
- draft-ietf-dnsext-dnssec-trustupdate-treshold

Operations

- draft-ietf-dnsop-dnssec-operations

NSEC++

- draft-arends-dnsnr
- draft-ietf-dnsext-nsec3
- draft-ietf-dnsext-trans

References and Acknowledgements

- www.dnssec.net
- www.dnssec-deployment.org
- www.ripe.net/disi/dnssec_howto
- “Is Hierarchical Public-Key Certification the Next Target for Hackers” can be found at:
<http://www.acmqueue.org/modules.php?name=Content&pa=showpage&pid=181>
- The participants in the dnssec-deployment working group provided useful feedback used in this presentation.
- This presentation contains material developed at RIPE NCC in cooperation with third parties.

Questions???

Ask

Research Areas

- Validators
- Key rollover methods
- User interfaces
- New DNS