DNSSEC

an introduction

ccTLD workshop
November 26-29th, 2007
Amman, Jordan

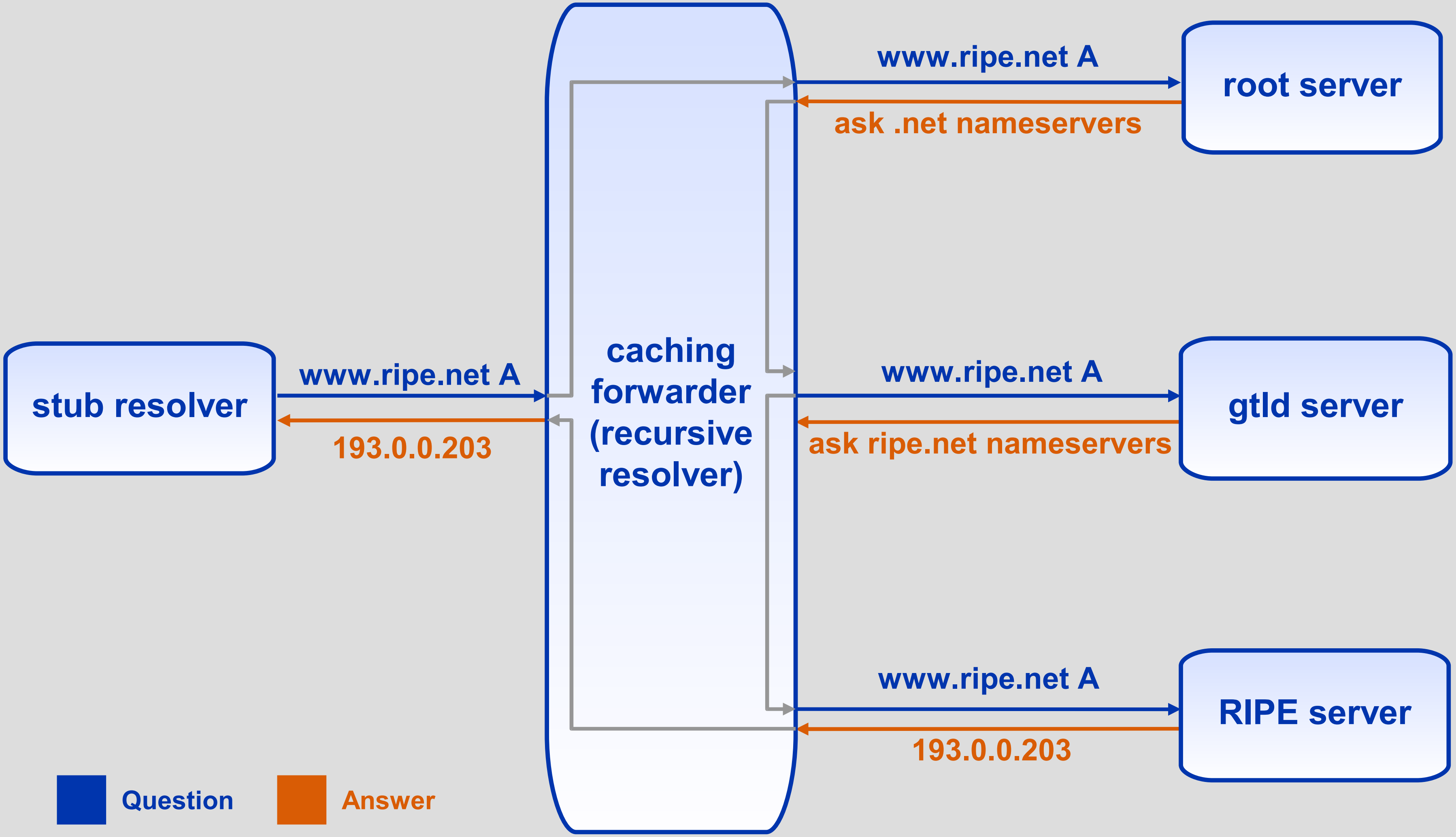
Based on slides from RIPE NCC

Overview

- DNS Vulnerabilities
- DNSSEC Mechanisms
  - New Resource Records
  - Setting Up a Secure Zone
  - Delegating Signing Authority
  - Key Rollovers
- Operational Concerns

DNS Vulnerabilities

DNS Resolving



stub resolver

www.ripe.net A

193.0.0.203

caching forwarder (recursive resolver)

www.ripe.net A

ask .net nameservers

root server

www.ripe.net A

ask ripe.net nameservers

gtld server

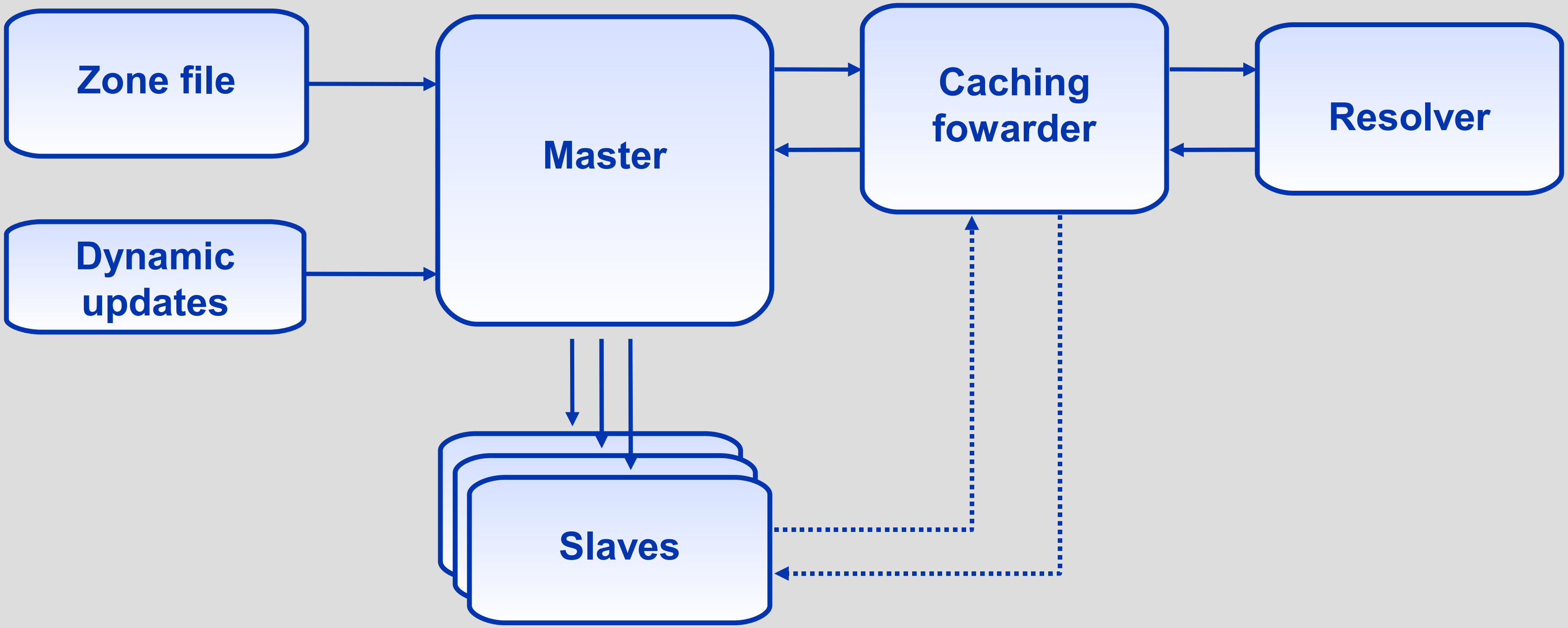
www.ripe.net A

193.0.0.203

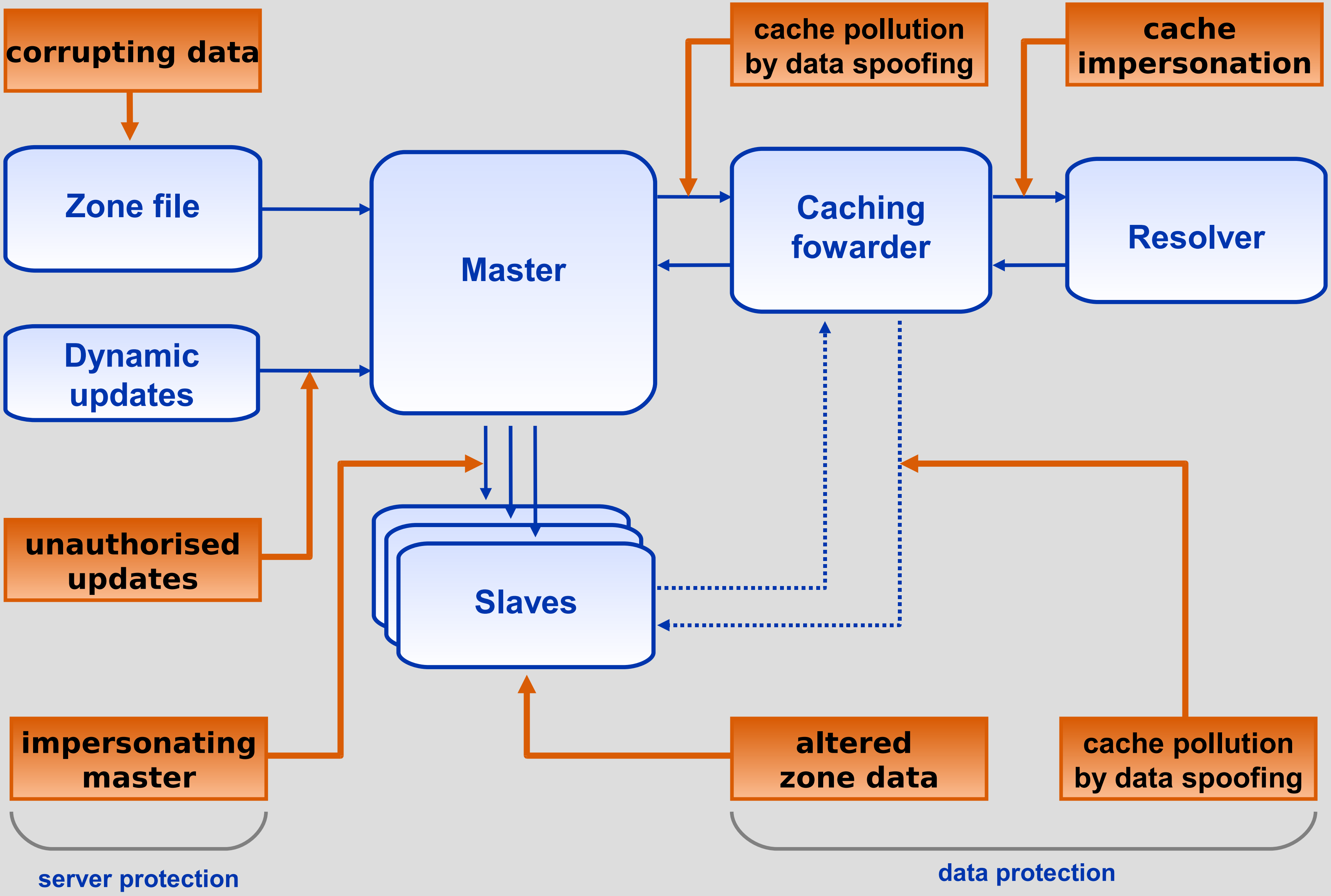
RIPE server

🟦 Question 🟧 Answer

DNS Data Flow

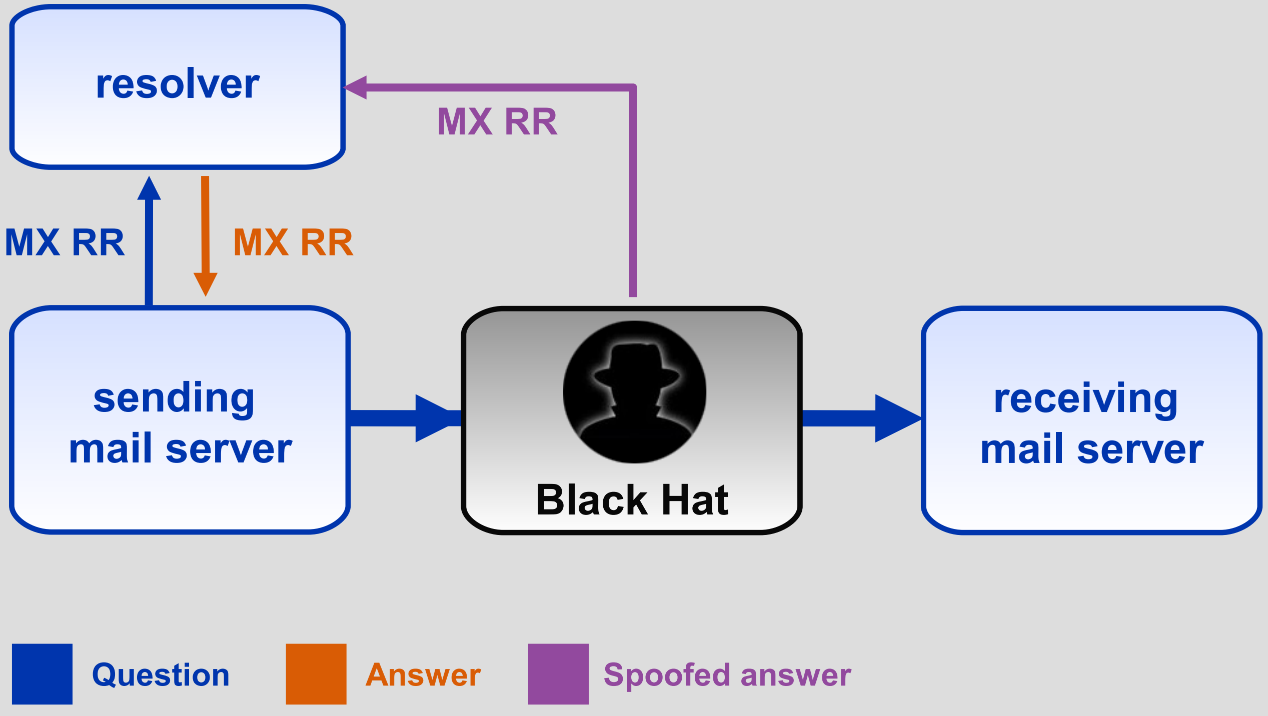


DNS Vulnerabilities



DNS Exploit Example

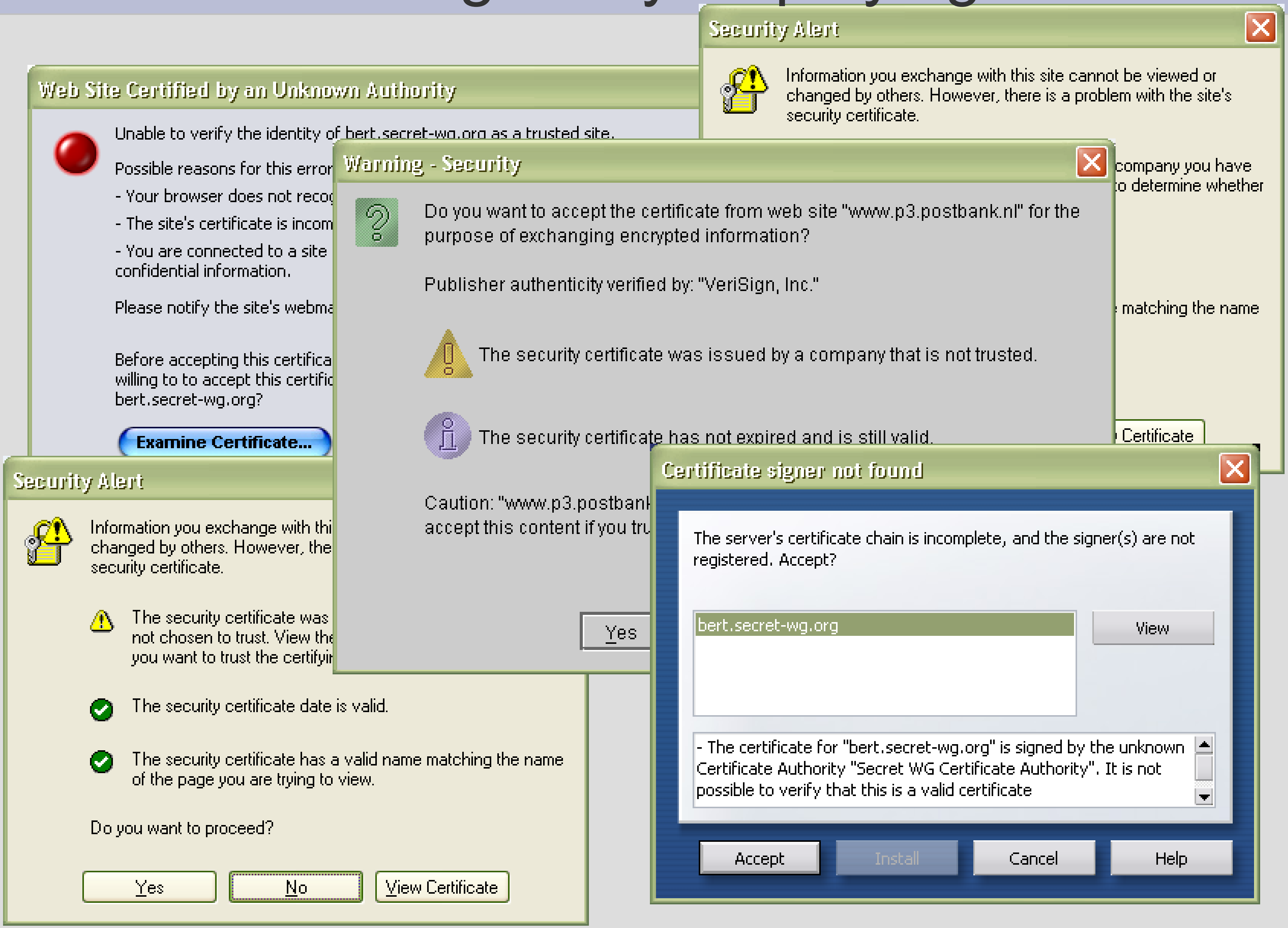
- Mail goes to the server in the MX resource record
- Path only visible in email headers



Other Possible DNS Targets

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

Mitigate by Deploying SSL?



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 recog
- The site's certificate is incom
- You are connected to a site confidential information.

Please notify the site's webma

Before accepting this certifica willing to to accept this certific bert.secret-wg.org?

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.

company you have to determine whether

matching the name

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 accept this content if you tru

Security Alert

Information you exchange with thi changed by others. However, the security certificate.

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

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?

Certificate signer not found

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

bert.secret-wg.org

- 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

Mitigate by Deploying SSL?

- Claim: SSL is not the magic bullet
  - (Neither is DNSSEC)
- Problem: Users are offered a choice
  - Far too often
  - Users are annoyed
- Implementation and use make SSL vulnerable
  - Not the technology

Where Does DNSSEC Come In?

- 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 from person from the one that does “DNSSEC”
  - The chains of trust are most probably different

DNSSEC Provides

- Data Origin Authentication
- Data Integrity
- Authenticating Name and Type Non-Existence

- DNSSEC
  - Is not designed to provide confidentiality
  - Provides no protection against denial of service attacks

DNSSEC Components

- TSIG/SIG(0): provides mechanisms to authenticate communication between machines
- DNSKEY/RRSIG/NSEC: provides mechanisms to establish authenticity and integrity of data
- DS: provides a mechanism to delegate trust to public keys of third parties

- A secure DNS will be used as an

Summary

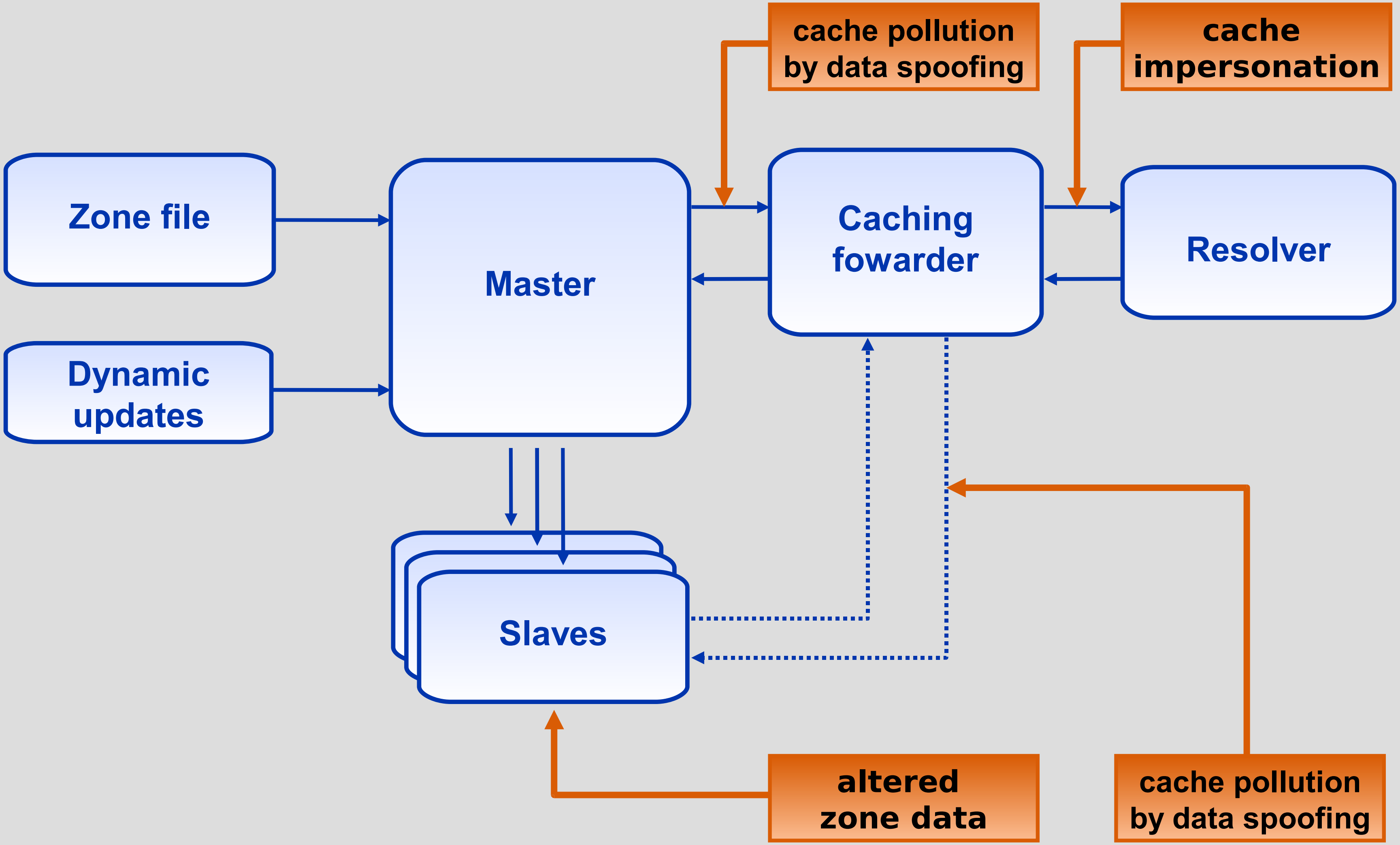
- DNS introduction
- DNS vulnerabilities
- SSL not the complete answer

Questions?

DNSSEC Mechanisms

- New Resource Records
- Setting Up a Secure Zone
- Delegating Signing Authority
- Key Rollovers

DNSSEC Protected Vulnerabilities



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)

DNSSEC summary

ripe.net.

```
www.ripe.net   IN 900 A 193.0.0.214
www.ripe.net   IN 900 RRSIG A ... 26523 ripe.net. ...

ripe.net       IN 3600 DNSKEY 256 3 5 ...
ripe.net       IN 3600 RRSIG DNSKEY ... 26523 ripe.net. ...
```

net.

```
ripe.net       IN 3600 DS 26523 5 1 ...
ripe.net       IN 3600 RRSIG DS .... 573 net. ...
```

Locally Configured Verifier (named.conf)

```
trusted-keys {  “ripe.net." 256 3 5 “...";  };
```

Security Status of Data (RFC4035)

- Secure
  - Resolver is able to build a chain of signed DNSKEY and DS RRs from a trusted security anchor to the RRset
- Insecure
  - Resolver knows that it has no chain of signed DNSKEY and DS RRs from any trusted starting point to the RRset
- Bogus
  - Resolver believes that it ought to be able to establish a chain of trust but for which it is unable to do so
  - May indicate an attack but may also indicate a configuration error or some form of data corruption
- Indeterminate
  - Resolver is not able to determine whether the RRset should be signed

New Resource Records

RRs and RRSets

- Resource Record:
  - name TTL class type rdata

```
www.ripe.net.   7200    IN  A   192.168.10.3
```

- RRset: RRs with same name, class **and** type:

```
www.ripe.net.   7200    IN  A   192.168.10.3
                    A   10.0.0.3
                    A   172.25.215.2
```

- RRSets are signed, not the individual RRs

New Resource Records

- Three Public key crypto related RRs
  - RRSIG Signature over RRset made using private key
  - DNSKEY Public key, needed for verifying a RRSIG
  - DS Delegation Signer; ‘Pointer’ for building chains of authentication

- One RR for internal consistency
  - NSEC Indicates which name is the next one in the zone and which typecodes are available for the current name
    - authenticated non-existence of data

NSEC Records

- NSEC RR provides proof of non-existence
- If the servers response is NXDOMAIN:
  - One or more NSEC RRs indicate that the name or a wildcard expansion does not exist
- If the servers response is NOERROR:
  - And empty answer section
  - The NSEC proves that the QTYPE did not exist
- More than one NSEC may be required in response
  - Wildcards
- NSEC records are generated by tools
  - Tools also order the zone

NSEC Walk

- NSEC records allow for zone enumeration
- Providing privacy was **not** a requirement
- Zone enumeration is a deployment barrier

- Work has started to study solutions
  - Requirements are gathered
  - If and when a solution is developed, it will co-exist with DNSSEC-BIS !

Summary

- DNSSEC not a PKI
- Zone status
- New RRs: DNSKEY, RRSIG, NSEC, DS

Questions?

Setting Up a secure Zone

Securing a Zone: Step 1

- Generate keypair
  - Include public key (DNSKEY) in zone file
  - dnssec-keygen tool comes with BIND

Securing a Zone: Step 2

- Sign your zone

- Signing will:
  - Sort the zone
  - Insert:
    - NSEC records
    - RRSIG records (signature over each RRset)
    - DS records (optional)
  - Generate key-set and ds-set files

Securing a Zone: Step 3

- Publish signed zone
- Signed zone is regular zonefile format
  - With extra resource records
- Make sure all your servers are DNSSEC capable!

Securing a Zone: Step 4

- Configure forwarding resolver
- Test
- DNSSEC verification only done in resolver!

Securing a Zone: Step 5

- Distribute your public key (DNSKEY)
  - To parent zone (key-set or ds-set can be used)
  - To everyone that wants/needs you as SEP

- Make sure to inform everyone of key rollovers!

Summary

- Generating keys
- Signing and publishing the zone
- Resolver configuration
- Testing the secure zone

Questions?

Delegating Signing Authority

Chains of Trust

Using the DNS to Distribute Keys

- 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

Key Problem

- Interaction with parent administratively expensive
  - Should only be done when needed
  - Bigger keys are better

- Signing zones should be fast
  - Memory restrictions
  - Space and time concerns
  - Smaller keys with short lifetimes are better

Key Functions

- Large keys are more secure
  - Can be used longer (□□
  - Large signatures => large zonefiles □□☎
  - Signing and verifying computationally expensive □□☎
- Small keys are fast
  - Small signatures□□□
  - Signing and verifying less expensive □□□
  - Short lifetime □□☎

Key solution: More Than One Key

- RRsets are signed, not RRs
- DS points to specific key
  - Signature from that key over DNSKEY RRset transfers trust to all keys in DNSKEY RRset
- Key that DS points to only signs DNSKEY RRset
  - Key Signing Key (KSK)
- Other keys in DNSKEY RRset sign entire zone
  - Zone Signing Key (ZSK)

Walking the Chain of Trust

Locally Configured

```
               Trusted Key . 8907
```

(root) .

```
.              DNSKEY (…) 5TQ3s… (8907) ; KSK
               DNSKEY (…) lasE5… (2983) ; ZSK

               RRSIG  DNSKEY (…)  8907 .  69Hw9…

net.           DS    7834 3 1ab15…
               RRSIG   DS (…) . 2983
```

net.

```
net.           DNSKEY (…) q3dEw… (7834) ; KSK
               DNSKEY (…) 5TQ3s… (5612) ; ZSK

               RRSIG  DNSKEY (…)  7834 net.  cMas…

ripe.net.      DS    4252 3 1ab15…
               RRSIG  DS (…) net. 5612
```

ripe.net.

```
ripe.net.      DNSKEY (…) rwx002…  (4252) ; KSK
               DNSKEY (…) sovP42…  (1111) ; ZSK

               RRSIG  DNSKEY (…) 4252 ripe.net.  5t...

www.ripe.net.  A 193.0.0.202
               RRSIG  A  (…)  1111 ripe.net.  a3...
```

Summary

- Scaling problem: secure islands
- Zone signing key, key signing key
- Chain of trust

Questions?

Key Rollovers

Key Rollovers

- Try to minimise impact
  - Short validity of signatures
  - Regular key rollover
- Remember: DNSKEYs do not have timestamps
  - the RRSIG over the DNSKEY has the timestamp
- Key rollover involves second party or parties:
  - State to be maintained during rollover
  - Operationally expensive

Key Rollover - Summary

1. Generate new KSK
2. Sign with old and new KSKs
3. Wait for your servers + TTL of old DNSKEY RRset
4. Inform resolvers of the new key
   - that have you as a trusted entry point

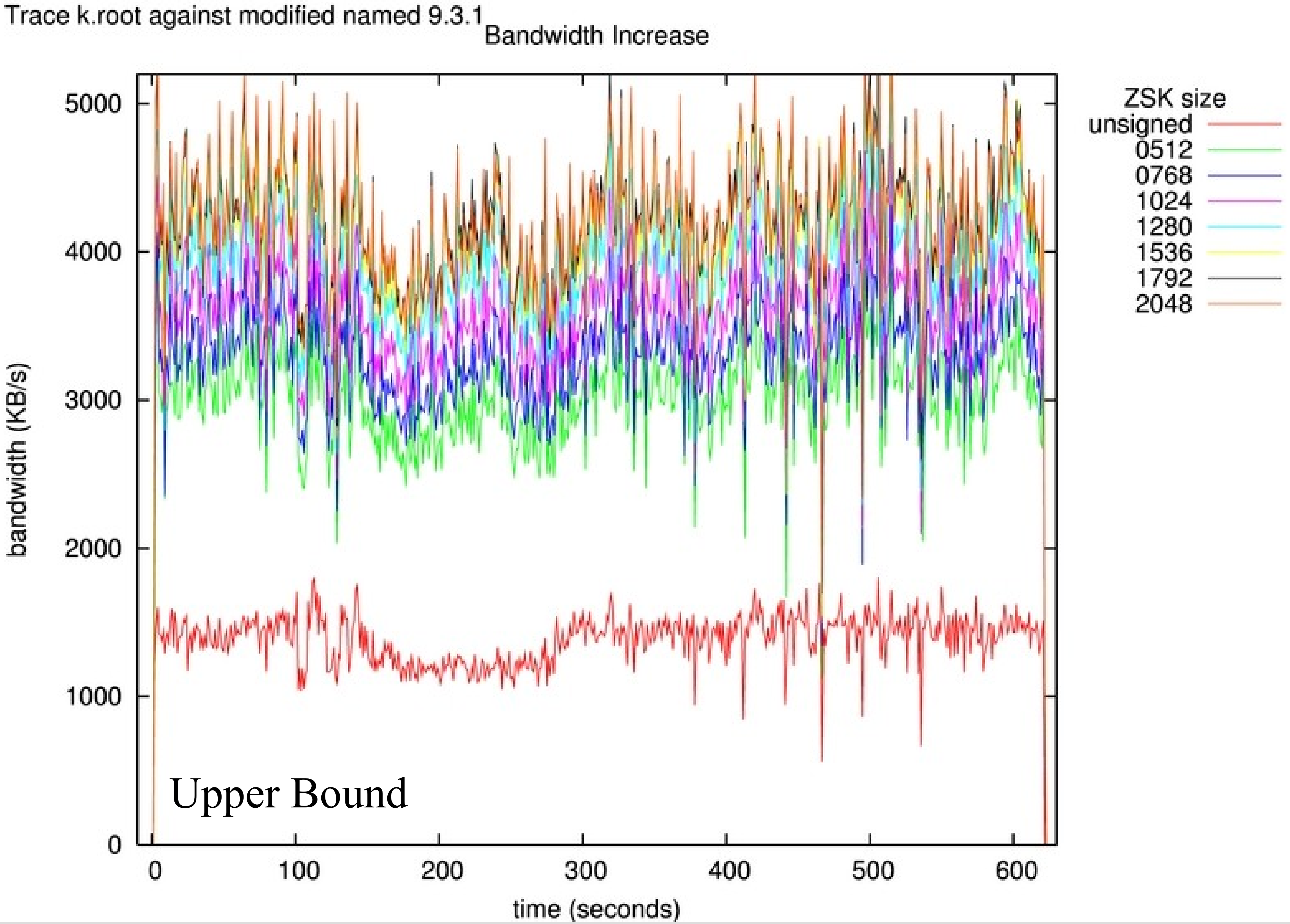
- Query for the parental DS and remember the TTL
- Upload the new KSK or DS to the parent
- Check if ***all*** parental servers have new DS
- Wait another TTL before removing the old key

Summary

- Key size and signature lifetimes
- Key rollovers
- Emergency procedure

Questions?

Operational Concerns


Trace k.root against modified named 9.3.1
Bandwidth Increase
bandwidth (KB/s)
5000
4000
3000
2000
1000
0
time (seconds)
0
100
200
300
400
500
600
ZSK size
unsigned
0512
0768
1024
1280
1536
1792
2048

Upper Bound

Operational Issues

- Increased memory, CPU & bandwidth usage
- Who signs the root zone?
  - IANA/ICANN
  - Department of Commerce
  - Verisign
- No system call for DNSSEC
- Local verifier on trusted network?
- End user choice?

Summary

- Increased memory and bandwidth demands
- “Political” issues

Questions?

The End!

Край

Y Diwedd

Fí

النهاية

Соңы

Վերջ

Finis

Liðugt

Ende

Кінець

Konec

Fund

پایان

Kraj

Son

Крај

Lõpp

Vége

An Críoch

הסוף

Endir

Fine

Sfârşit

Fin

Τέλος

Einde

Конец

Slut

Slutt

დასასრული

Pabaiga

Tmiem

Koniec

Amaia

Loppu

Fim