

# DNSSEC technical overview

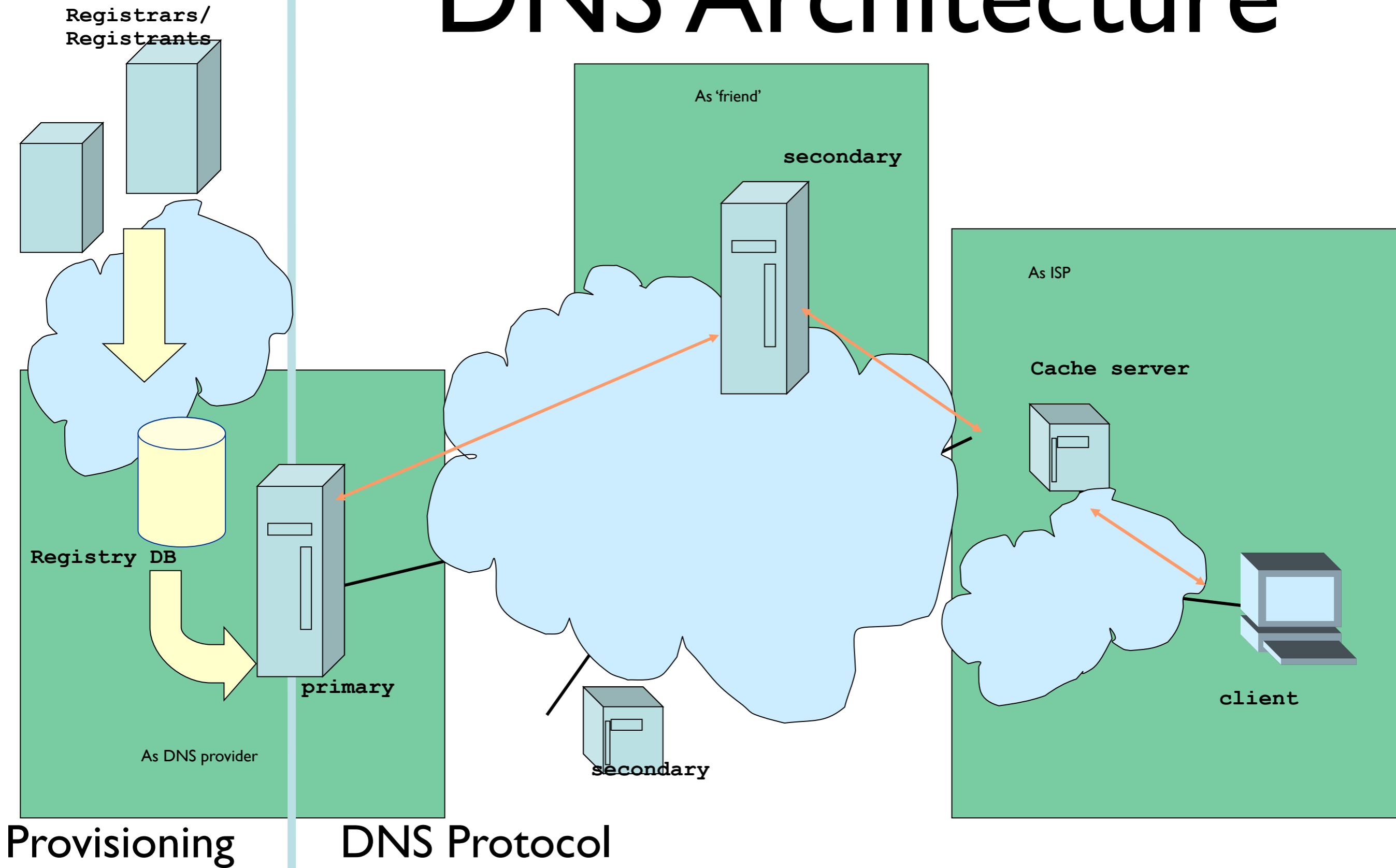
Alain Patrick AINA [aalain@trstech.net](mailto:aalain@trstech.net)



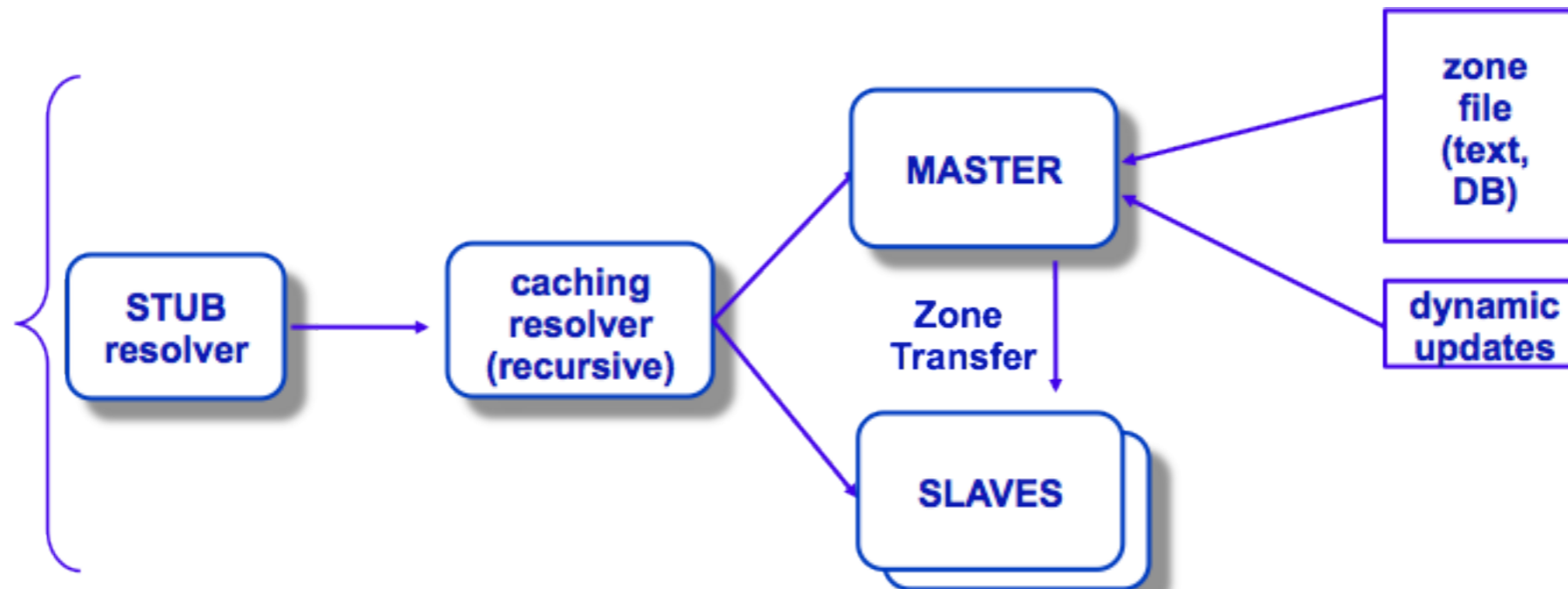
# Objectives

- Understand DNSSEC terminology
- Understand the threat models that DNSSEC is intended to address
- Appreciate the benefits of DNSSEC to sensitive applications
- Understand some of the operational and legal implications of DNSSEC

# DNS Architecture

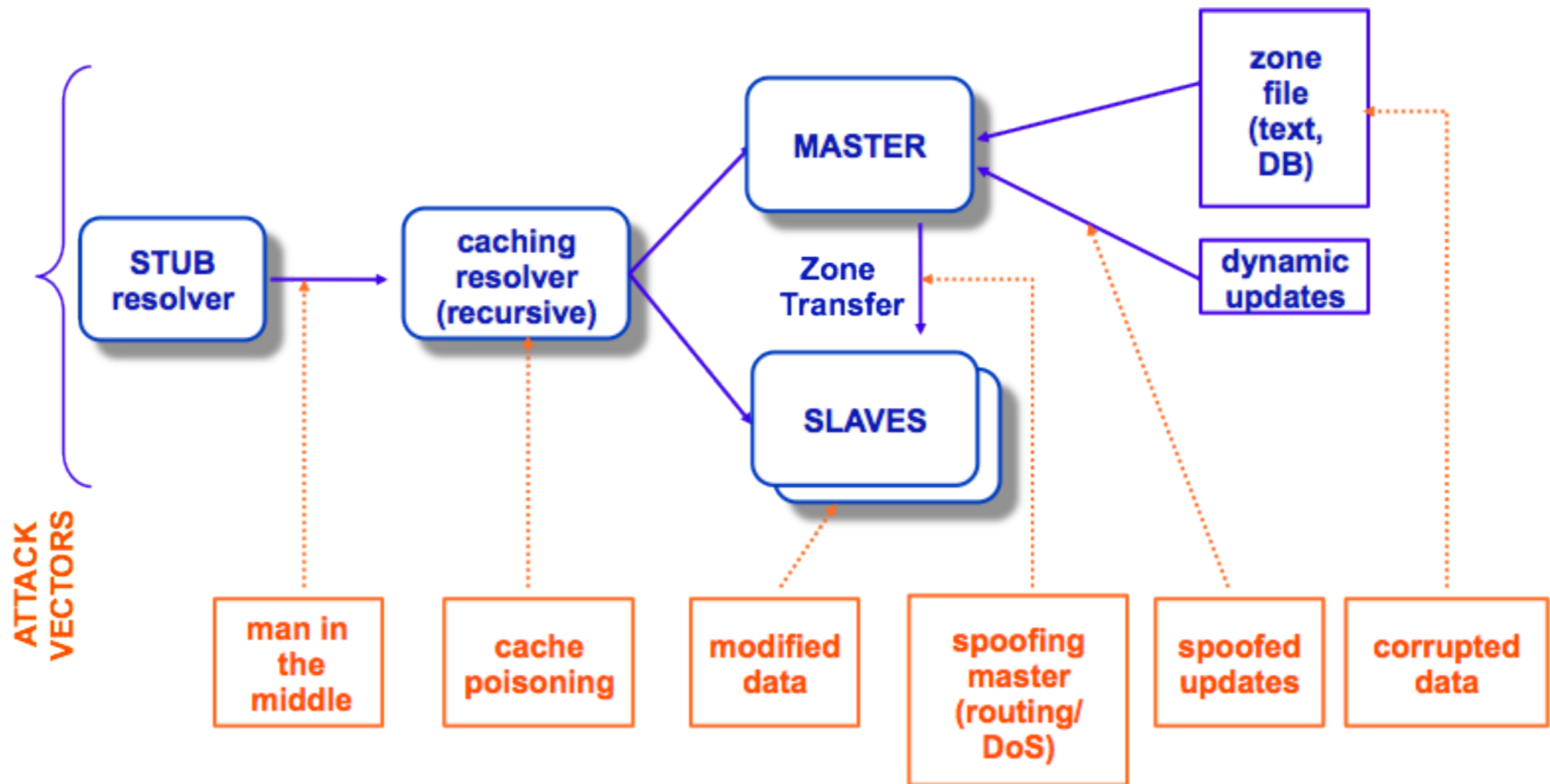


# DNS Data Flow

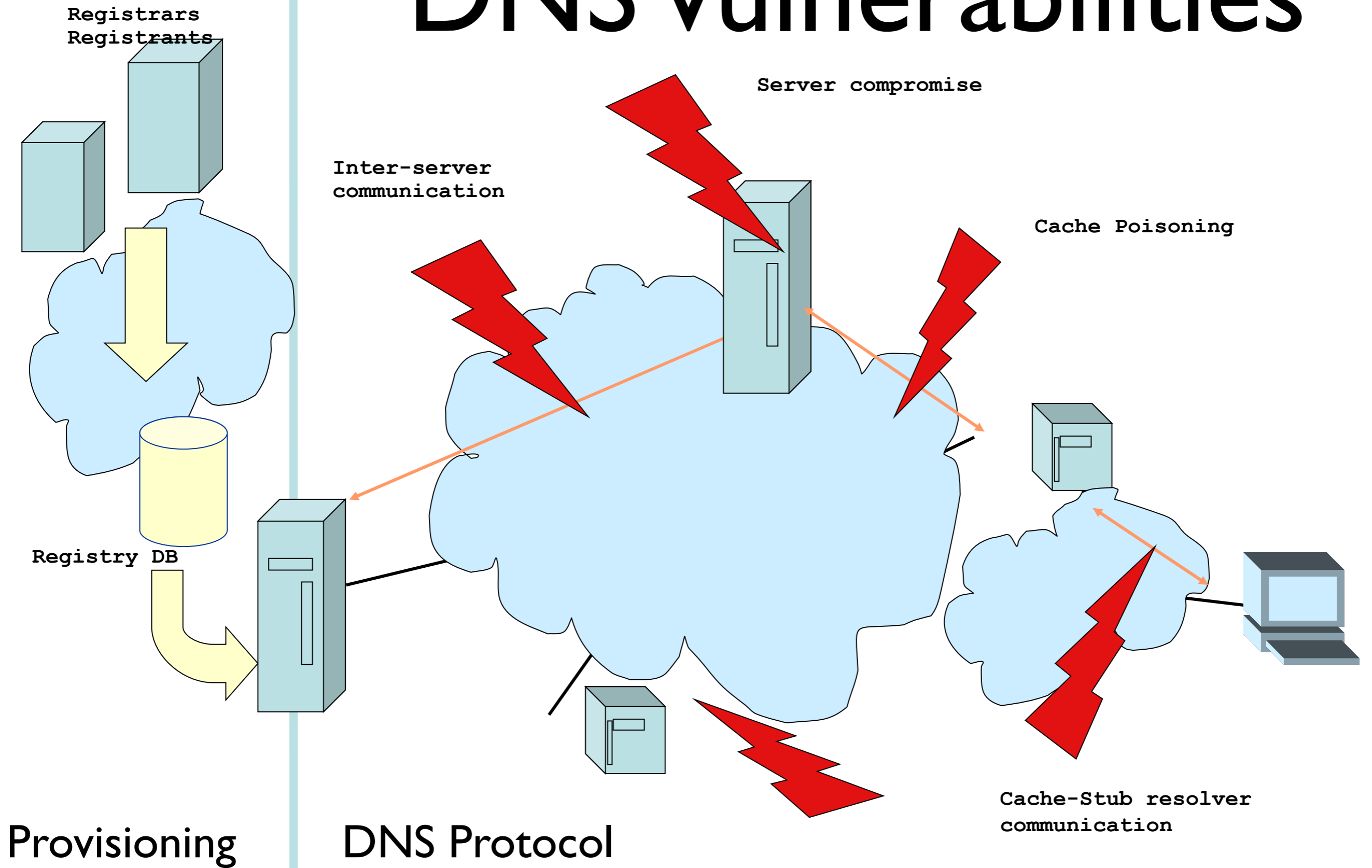


# DNS Vulnerabilities

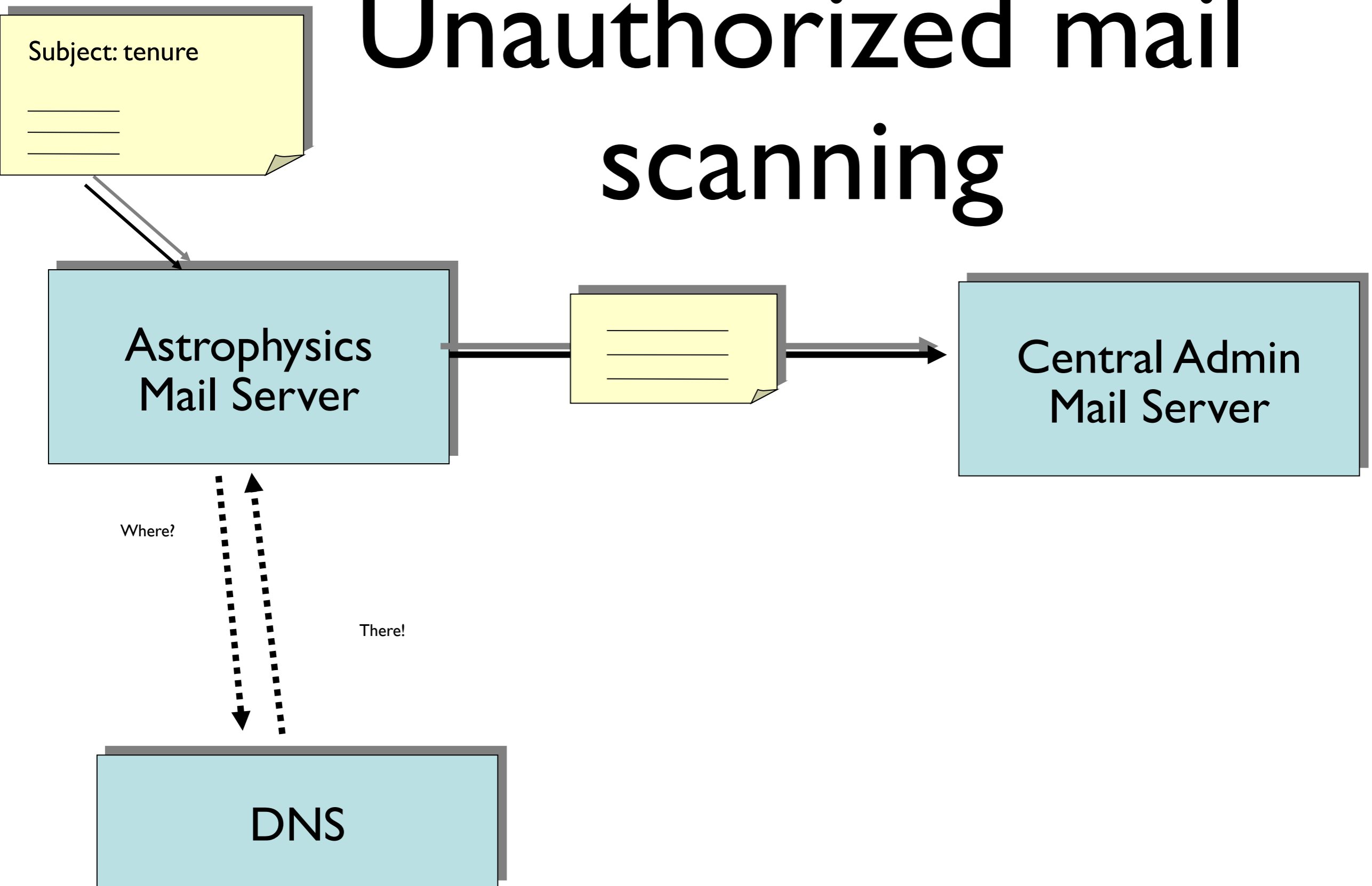
# DNS Vulnerabilities



# DNS Vulnerabilities

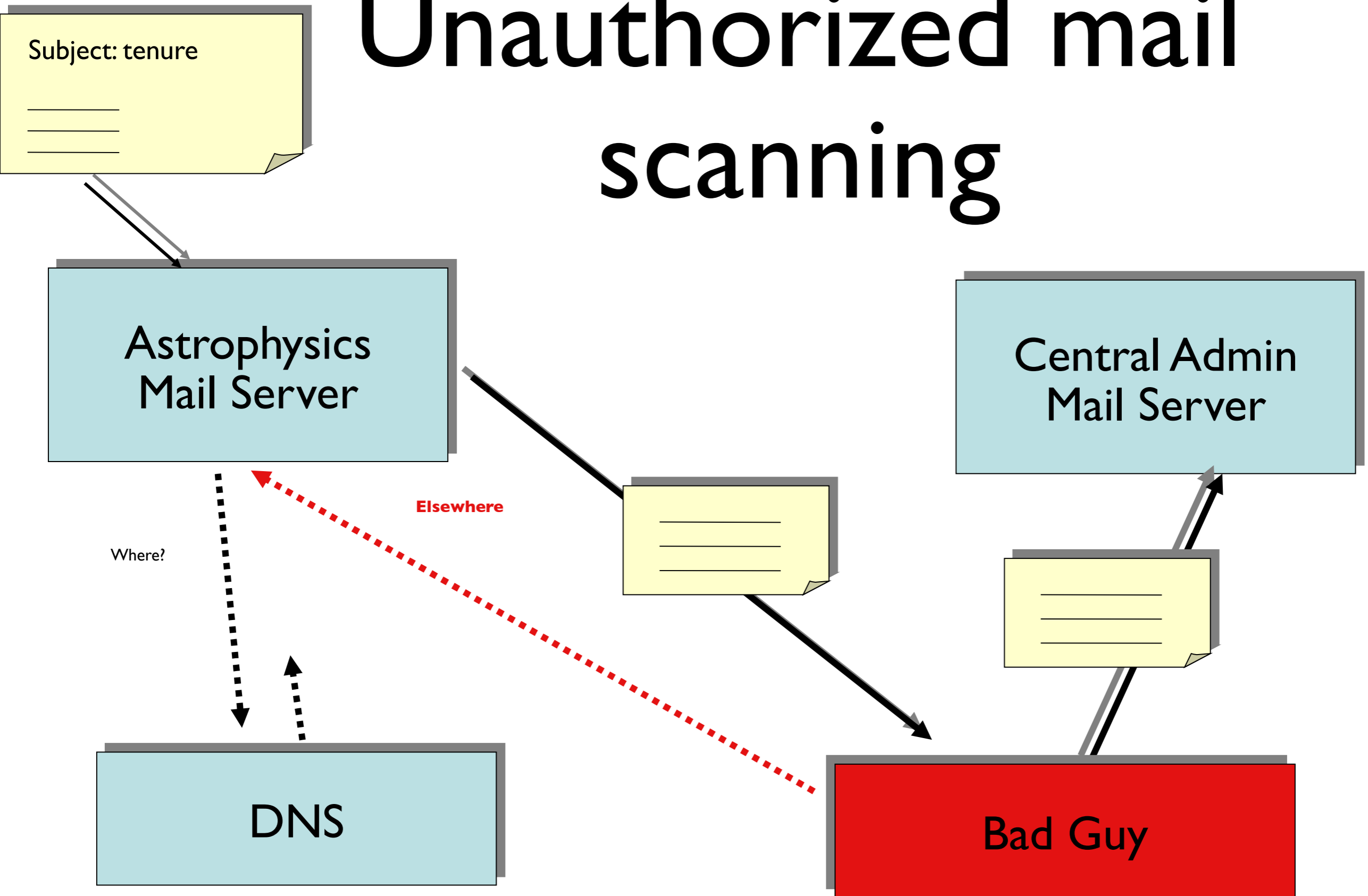


# Example: Unauthorized mail scanning

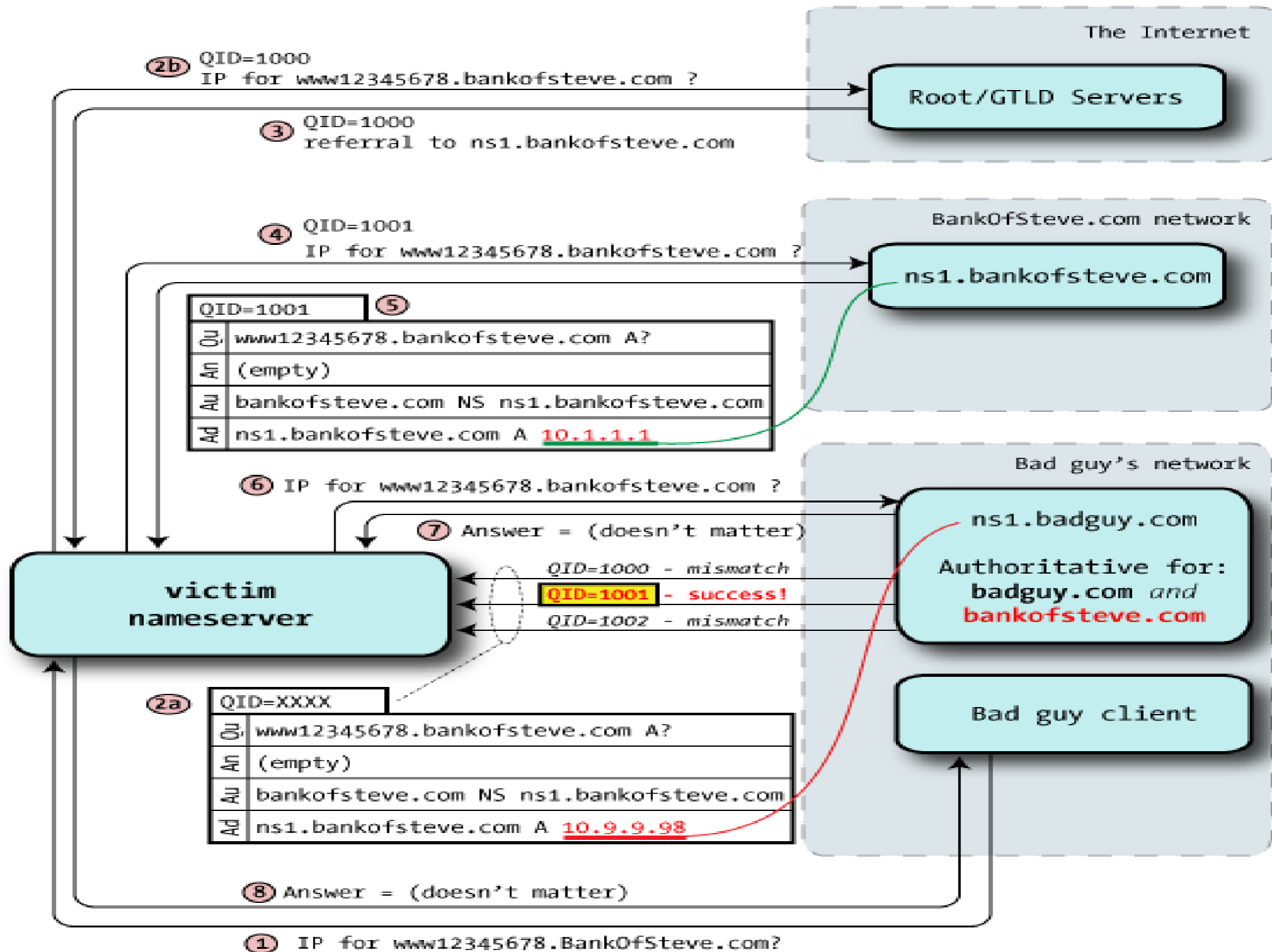




# Example: Unauthorized mail scanning



# Kaminsky attack



# Kaminsky attack (con't)

The screenshot shows the Metasploit website interface. At the top left is the Metasploit logo. To the right, there are links for 'Stay Updated | Metasploit Blog | Website Feedback' and a search bar with the placeholder text 'search for keyword'. Below the search bar is a navigation menu with items: Home, ABOUT, HELP, NEWS, DEVELOPMENT, EXPLOITS, WEAR SWAG, DOWNLOAD, and READ THE FORUMS. The 'DOWNLOAD' item is highlighted in yellow. Below the navigation menu, the breadcrumb 'Home > Exploit DB' is visible. The main heading is 'DNS BailiWicked Domain Attack'. The description states: 'This exploit attacks a fairly ubiquitous flaw in DNS implementations which Dan Kaminsky found and disclosed ~Jul 2008. This exploit replaces the target domains nameserver entries in a vulnerable DNS cache server. This attack works by sending random hostname queries to the target DNS server coupled with spoofed replies to those queries from the authoritative nameservers for that domain. Eventually, a guessed ID will match, the spoofed packet will get accepted, and the nameserver entries for the target domain will be replaced by the server specified in the NEWDNS option of this exploit.' Below the description is a blue button labeled 'SEARCH OTHER MODULES >'. To the right of the main content is a grey box with the text 'GET METASPLOIT FOR PENETRATION TESTING' and a yellow button labeled 'FREE DOWNLOAD'. Below the description, there are sections for 'Rank' (Normal), 'Authors' (l)ruid < druid [at] caughtq.org >, hdm < hdm [at] metasploit.com >, Cedric Blancher < sid [at] rstack.org >, and 'Vulnerability References' (CVE-2008-1447, OSVDB-46776, US-CERT-VU-800113, http://www.caughq.org/exploits/CAU-EX-2008-0003.txt).

metasploit®

Stay Updated | Metasploit Blog | Website Feedback

Search search for keyword

Home > Exploit DB

## DNS BailiWicked Domain Attack

This exploit attacks a fairly ubiquitous flaw in DNS implementations which Dan Kaminsky found and disclosed ~Jul 2008. This exploit replaces the target domains nameserver entries in a vulnerable DNS cache server. This attack works by sending random hostname queries to the target DNS server coupled with spoofed replies to those queries from the authoritative nameservers for that domain. Eventually, a guessed ID will match, the spoofed packet will get accepted, and the nameserver entries for the target domain will be replaced by the server specified in the NEWDNS option of this exploit.

SEARCH OTHER MODULES >

### Rank

Normal

### Authors

l)ruid < druid [at] caughtq.org >  
hdm < hdm [at] metasploit.com >  
Cedric Blancher < sid [at] rstack.org >

### Vulnerability References

CVE-2008-1447  
OSVDB-46776  
US-CERT-VU-800113  
<http://www.caughq.org/exploits/CAU-EX-2008-0003.txt>

GET METASPLOIT FOR  
PENETRATION  
TESTING

FREE DOWNLOAD

# Reflection Attacks

- DNS servers can act as very efficient packet amplifiers
- Use of UDP, small queries, large responses
- DNSSEC makes DNS servers *better* packet amplifiers
- Still lots of UDP, larger responses

# Reliability

- In the grand scheme of things, DNSSEC does not help make your DNS more reliable
- in fact it makes the DNS more brittle, and makes it harder to maintain reliable service

# Confidentiality

- DNSSEC does not address confidentiality of queries or responses
- anybody who can intercept a secure response can still see the details
- there is no *encryption* here

# Integrity, Authenticity

- DNSSEC provides a mechanism for *data* published in the DNS to carry cryptographic signatures
- secure responses include signatures
- clients receiving a secure response can tell whether it is authentic

# Benefits of DNSSEC



# 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

# DNSSEC secondary benefits

- 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](http://acmqueue.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”

# More benefits?

- *DNS-based Authentication of Named Entities WG*

<http://tools.ietf.org/wg/dane/>

## **Objective:**

**Specify mechanisms and techniques that allow Internet applications to establish cryptographically secured communications by using information distributed through DNSSEC for discovering and authenticating public keys which are associated with a service located at a domain name.**

# Attacks against PKI

The screenshot shows a web browser window with the URL [http://threatpost.com/en\\_us/blogs/attackers-obtain-valid-cert-google-domains-mozilla-moves-revoke-it-082911](http://threatpost.com/en_us/blogs/attackers-obtain-valid-cert-google-domains-mozilla-moves-revoke-it-082911). The page is from threatpost.com and is part of the Kaspersky Lab Security News Service. The article is dated August 29, 2011, at 7:31 PM. The title is "Attackers Obtain Valid Cert for Google Domains, Mozilla Moves to Revoke It" by Dennis Fisher. The article text includes an update about a certificate authority in the Netherlands issuing a valid SSL wildcard certificate for Google, which was later revoked by DigiNotar. The article also mentions that the attack targeted Gmail users and that the certificate was posted to Pastebin. A sidebar on the right lists "Today's Most Popular" articles, including "60 Minutes Weighs Stuxnet's Legacy" and "Google Patches 14 Chrome Bugs Ahead of Pwn2Own, Pays \$30k in Special Rewards". At the bottom of the page, there is a promotional banner for "Security for Virtualization in 2 minutes" with a link to watch an animation.

Attacker's Obtain Valid Cert for Google Domains, Mozilla Moves to Revoke It | threatpost

Router Allo...sco Systems Cisco IOS Se...sco Systems network aut...rche Google http://www...mniPCX.pdf ISOC-AU Submissions End-of-Sale...sco Systems Corporate ti...ncyclopedia

Attackers Obtain Valid Cert for G... Capture a Screen Shot with Mac OS X

The Kaspersky Lab Security News Service

Apple | Cloud | Compliance | Critical Infrastructure | Cryptography | Government | Hacks | Malware

Microsoft | Mobile Security | SMB | Social Engineering | Virtualization | Vulnerabilities | Web Security

Home › SMB Security ›

August 29, 2011, 7:31PM

## Attackers Obtain Valid Cert for Google Domains, Mozilla Moves to Revoke It

by Dennis Fisher

Follow @DennisF

Twitter Facebook +1 Share Like 16

+1 0 Comment

**UPDATE:** A certificate authority in the Netherlands issued a valid SSL wildcard certificate for Google to a third party in July, leading to concerns that attackers may have been using the certificate to route sensitive traffic through their own servers, capturing it and compromising user data in the process. The certificate was revoked by the CA, DigiNotar, after the problem came to light Monday and Mozilla and Microsoft both have removed DigiNotar from their lists of trusted root CAs.

The attack appears to have been targeting Gmail users specifically. Some users trying to reach the Gmail servers over HTTPS found that their traffic was being rerouted through servers that shouldn't have been part of the equation. On Monday afternoon, security researcher Moxie Marlinspike checked the signatures on the certificate for the suspicious server, which had been [posted to Pastebin](#) and elsewhere on the Web, and found that the certificate was in fact valid. The attack is especially problematic because the certificate is a wildcard cert, meaning it is valid for any of Google's domains that use SSL.

It's not clear who DigiNotar issued the certificate to at this point.

Security and privacy experts began discussing the problem Monday

### Security for Virtualization

in 2 minutes

Get the right balance between security and performance with our animated video

▶ Watch the animation now

# Attacks against PKI(cont.)

The screenshot shows a web browser window displaying a Threatpost article. The browser's address bar shows the URL: [http://threatpost.com/en\\_us/blogs/microsoft-revokes-trust-five-diginotar-root-certs-090611](http://threatpost.com/en_us/blogs/microsoft-revokes-trust-five-diginotar-root-certs-090611). The page title is "Microsoft Revokes Trust in Five DigiNotar Root Certs, Mozilla Drops Trust For Staat der Nederland Certs | threatpost". The Threatpost logo is visible, along with the tagline "The Kaspersky Lab Security News Service". The article is dated "Monday, March 5th, 2012". The main headline of the article is "Microsoft Revokes Trust in Five DigiNotar Root Certs, Mozilla Drops Trust For Staat der Nederland Certs", written by Dennis Fisher on September 6, 2011, at 1:37PM. The article text begins with "The fallout from the [DigiNotar compromise](#) continued on Tuesday, as [Microsoft said it has now revoked its trust](#) of all five of the certificate authority's root certificates. The update that makes this change is being pushed out to users on all supported versions of Windows. Mozilla also released new versions of Firefox on Tuesday that revoke trust for all of DigiNotar's certificates." The article also mentions that the move by Microsoft effectively makes any certificate issued by DigiNotar untrusted by Internet Explorer and other Windows applications. A sidebar on the right titled "Today's Most Popular" lists several security-related articles, including "60 Minutes Weighs Stuxnet's Legacy", "Google Patches 14 Chrome Bugs Ahead of Pwn2Own, Pays \$30k in Special Rewards", "NSA Develops New, Super-Secure Android Phone", "Threats From Third Party Vendors Demand Vigilance", and "Former NSA Director Calls Stuxnet 'Good Idea'". There is also a promotional banner for "Security for Virtualization" in 2 minutes.

Microsoft Revokes Trust in Five DigiNotar Root Certs, Mozilla Drops Trust For Staat der Nederland Certs | threatpost

http://threatpost.com/en\_us/blogs/microsoft-revokes-trust-five-diginotar-root-certs-090611

Monday, March 5th, 2012

threatpost  
The Kaspersky Lab Security News Service

Apple | Cloud | Compliance | Critical Infrastructure | Cryptography | Government | Hacks | Malware  
Microsoft | Mobile Security | SMB | Social Engineering | Virtualization | Vulnerabilities | Web Security

Home > SMB Security >

September 6, 2011, 1:37PM

## Microsoft Revokes Trust in Five DigiNotar Root Certs, Mozilla Drops Trust For Staat der Nederland Certs

by Dennis Fisher  
Follow @DennisF

1 Comment

The fallout from the [DigiNotar compromise](#) continued on Tuesday, as [Microsoft said it has now revoked its trust](#) of all five of the certificate authority's root certificates. The update that makes this change is being pushed out to users on all supported versions of Windows. Mozilla also released new versions of Firefox on Tuesday that revoke trust for all of DigiNotar's certificates.

The move by Microsoft effectively makes any certificate that has been issued by DigiNotar untrusted by Internet Explorer and other Windows applications. Any IE user who visits a site that presents a DigiNotar-issued certificate as proof of identity will get an error message telling him that the certificate isn't trusted. Microsoft's change applies to these root certificates from DigiNotar:

### Today's Most Popular

- 60 Minutes Weighs Stuxnet's Legacy
- Google Patches 14 Chrome Bugs Ahead of Pwn2Own, Pays \$30k in Special Rewards
- NSA Develops New, Super-Secure Android Phone
- Threats From Third Party Vendors Demand Vigilance
- Former NSA Director Calls Stuxnet "Good Idea"

### Security for Virtualization

in 2 minutes

Get the right balance between security and performance with our animated video

# Benefits to End-Users

- Users who validate will not see answers from the DNS that fail validation
  - might increase helpdesk load, but the alternative is infected computers, stolen bank details, etc
- Ongoing work to improve SSL security using DNSSEC-signed certificates
  - IETF “dane” working group

# Benefits to Content Providers

- Reduce the risk that your content is being intercepted by unknown third parties
  - for end-users that validate, at least
- Demonstrate technical proficiency and security awareness



# Three Slides about Cryptography

# Cryptography

- Public Key Cryptography
  - X.509, PGP, ssh, DNSSEC
- (Public, Private) Key Pairs
  - use the private key to sign data
  - use the public key to verify signature

# Private Key

- The private key needs to be kept private and secure
  - the degree of security depends on what the key is used for
  - a compromised key means you can no longer expect people to trust signatures
  - a signature from a compromised key is more dangerous than no signature at all

# Public Key

- The public key needs to be widely-distributed
  - it also needs to be accurate
- In DNSSEC, public keys are published as DNSKEY RRSets in the zone they are used to sign
- Trust anchors are published in the parent zone as DS RRSets

# DNSSEC Protocol

# DNS Considerations

- When using the DNS to distribute keys, we need to remember a few things
  - the DNS is widely-distributed
  - information does not update instantaneously
  - we need to think hard about TTLs and caches when constructing a suitable policy

# Public Keys in the DNS

- In DNSSEC, we distribute public keys in the DNS itself
  - use the DNSKEY RRSet
  - supports different key sizes, cryptographic algorithms

# RR Signing in DNSSEC

- Each Resource Record Set (RRSet) can carry zero or more signatures
- signatures appear in an RRSIG RRSet with the same owner name
- signatures have an inception and expiry time
  - we need to re-sign regularly



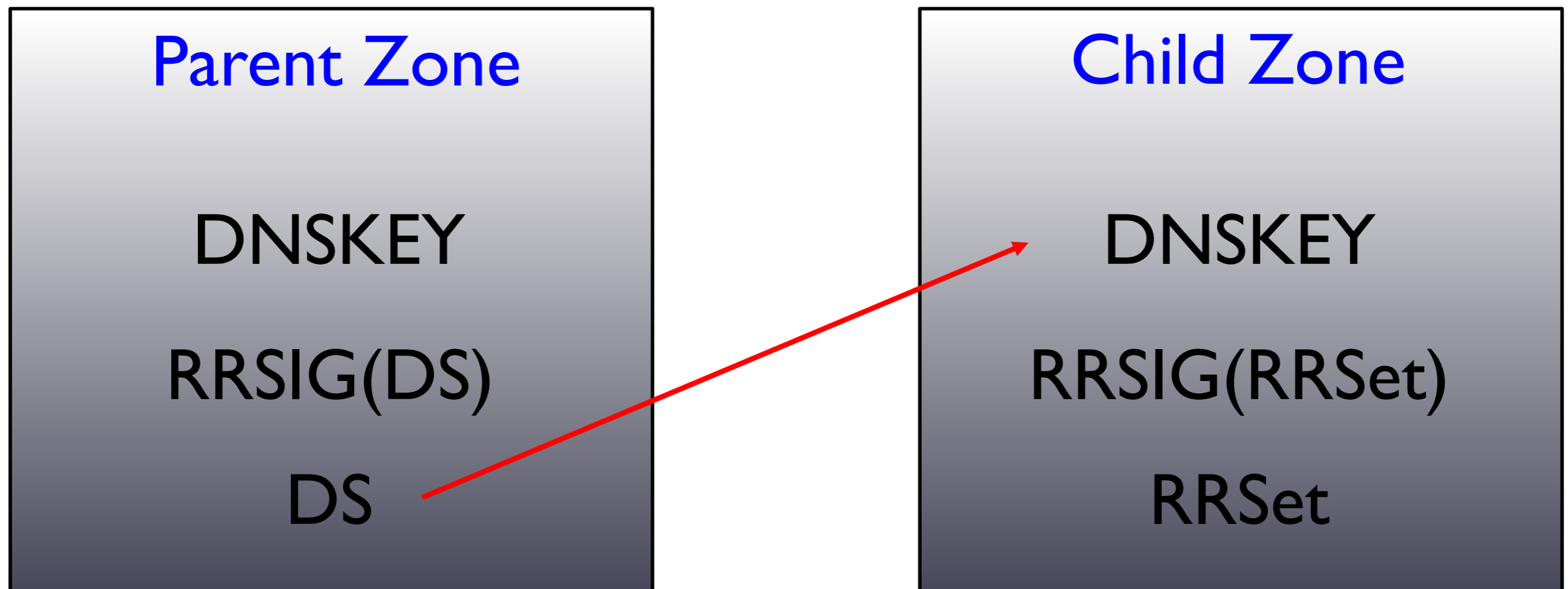
# Chain of Trust

- If we can trust the public key which corresponds to the private key that made a signature, we can trust a signature
- If we can trust a signature, we can trust the data that is signed
- How do we trust the public key?

# Delegation Signer

- DS is the Delegation Signer Resource Record
  - it carries a hash of a public key
  - it is signed
  - this is how we extend trust across delegations

# Chain of Trust



# Chain of Trust



# Root Anchor

- At some point a validator needs to install a trust anchor into its software
  - root zone trust anchor
  - <http://www.iana.org/dnssec/>

# Two DNSKEY RRsets

- Common practice is to use two different DNSKEY RRsets per zone
  - ZSK – Zone Signing Key
    - used to sign the data in the zone
  - KSK – Key Signing Key
    - used to sign the DNSKEY RRSet

# ZSK

- Since we need to re-sign the zone regularly, the ZSK needs to be on-line
- The ZSK is the key that is used most often by validators, so we can make it smaller and save some CPU
- We can change the ZSK we are using regularly without involving others

# KSK

- The KSK is the key that corresponds to the DS record in our parent zone
- We need to use the KSK to sign the ZSK, and then we can put it away in a safe place
- no need to keep the KSK on-line
- changing the KSK involves talking to our parent (update DS record)



# KSK and ZSK

## Parent Zone

DNSKEY(KSK)

DNSKEY(ZSK)

RRSIG(DNSKEY)

RRSIG(DNSKEY)

RRSIG(DS)

DS

## Child Zone

DNSKEY(KSK)

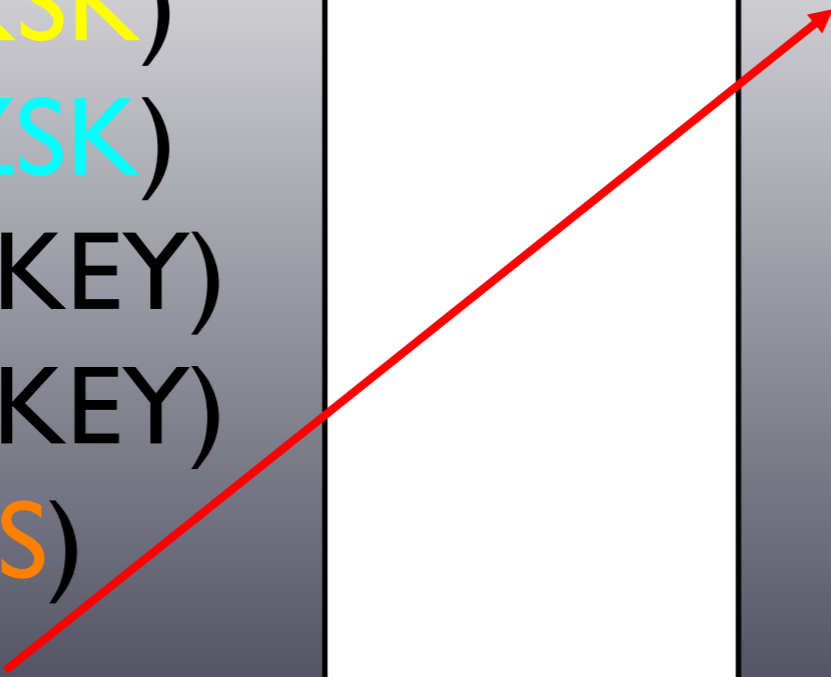
DNSKEY(ZSK)

RRSIG(DNSKEY)

RRSIG(DNSKEY)

RRSIG(RRSet)

RRSet



# DNS Transport

- Plain old DNS was optimised to work over UDP with small packets (512 bytes)
  - fall-back to TCP
- Modern DNS supports larger messages over UDP (EDNS0, RFC 2671)
- DNSSEC means larger DNS messages
  - beware of faulty assumptions in firewalls!
    - Cisco PIXes and ASA can still cause problems with "fixup"

# Signing Things that Are Not There

- Verifiable deniability of existence
  - you can't sign something that's not there
  - use NSEC or NSEC3 records to cover the gaps
  - sign the NSEC and NSEC3 records
    - More on this later...

# DNSSEC for ISPs

# Validate

- The most effective step you can take to encourage DNSSEC uptake as an ISP is to validate responses
- DNSSEC-signed zones are fairly new, so expect this to cause some non-zero (but manageable) amount of helpdesk load
- Comcast is an example of a large ISP (in the US) who has taken this step

# DNSSEC for Registries and Hosting Providers

# Sign your Zones

- All the zones you serve can be signed
  - think about key rollover
  - think about key compromise scenarios, and what processes you will follow when you detect them
  - think about how you can detect compromises, and monitor signatures

# Key Management

- need to implement secure key storage, management procedures
- need to sign your zones
- registries need to accept DS records from users (how?)
- need to publish DS records to parents (how?)



# NSEC and NSEC3

- If you're signing a zone, you have to use one of these. Which one?
- Simple rule of thumb
  - if you are happy for anybody in the world to obtain a copy of your zone, and your zone is not very big, use NSEC
  - if you normally don't allow (e.g.) zone transfers to random people, or if you have a large zone to sign, use NSEC3

# Key Management

- DNSSEC has many parameters to consider, including:
  - key rollover schedule
  - signature duration
  - choosing appropriate TTL for the zone data
  - key size
- Those will be determined by *your policy*
- You must determine them for your own organisation, via a risk and operational assessment
- Don't blindly copy the policies of another organisation

# Key Management

- How do we keep the ZSK secure?
- How do we keep the KSK secure?
  - important questions
  - no simple answers here
  - requires risk analysis, consultation, maybe audit
  - again, a matter of policy
    - hybrid models possible
      - HSM for KSK, software for ZSK

# Communication

- Communicate with your customers
  - explain benefits/risks of DNSSEC
- Communicate with end-users
  - demonstrate how to validate responses
  - explain operational changes (firewalls, TCP, response sizes)

# Legal Aspects

# Legal Aspects

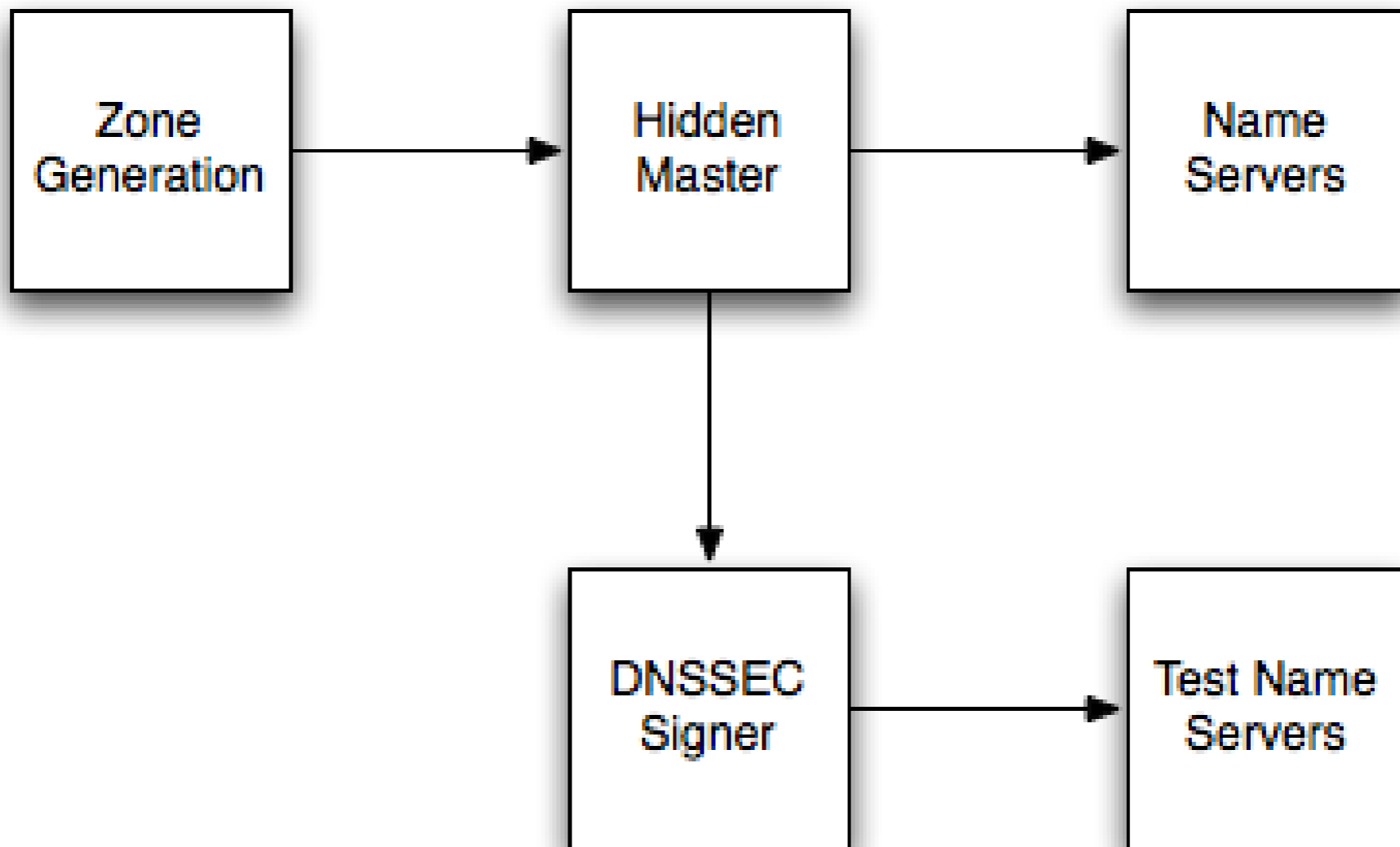
- Deployment of DNSSEC involves trust in procedures and policies
  - otherwise why trust signatures?
- DNSSEC Policy and Practice Statement (DPS)
  - a public attestation of procedures and policies
  - can be used as the basis for audits

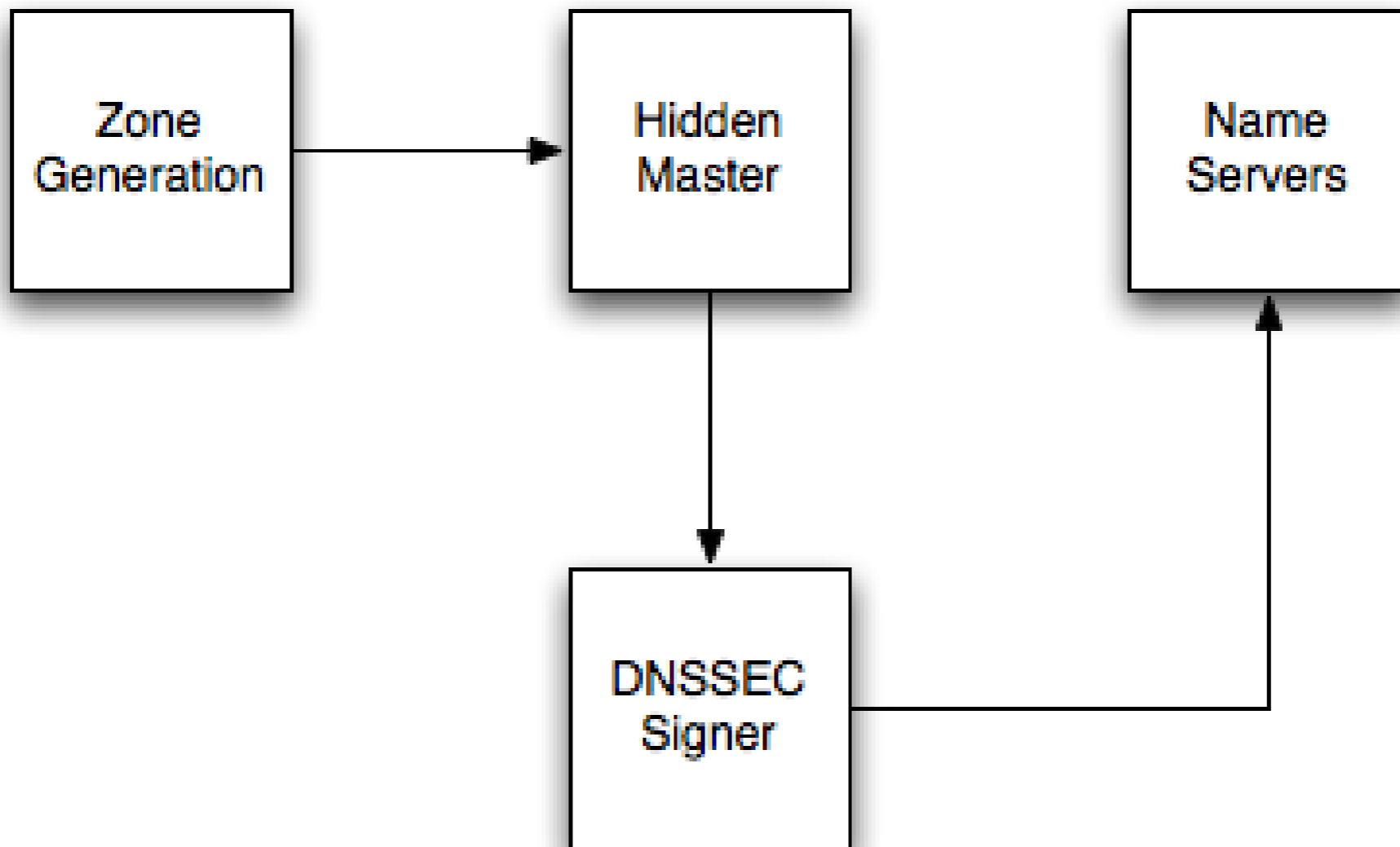
# Migration Strategies for Registries and DNS Hosting Companies

# Migration

- For registries and hosting providers, DNSSEC can be deployed without radically changing your existing systems
- registries will need to deploy a means of publishing trust anchors as DS RRsets, however







# Streamlined Operations

- Remember, DNSSEC makes you zones more brittle and fragile than they were before
- need to have excellent reliability in registry and DNS operations (verification of output, monitoring, etc...)
- need to have emergency procedures to update DS RRsets in your zones

# Resources

# Open-Source Software

- NSD
  - <http://www.isc.org/>
- BIND9
  - <http://www.isc.org/>
- Unbound
  - <http://www.unbound.net/>
- OpenDNSSEC
  - <http://www.opendnssec.org/>

# Mailing Lists

- dnssec-deployment mailing list
  - <http://www.dnssec-deployment.org/>
- dns-operations mailing list
  - <http://www.dns-oarc.net/>
- Ongoing protocol work
  - IETF dnsop, dnsext working groups

# Other resources

- DNS visualization tool

<http://dnsviz.net>

- DNSSEC AFRICA

<http://dnssec-africa.org>

# DPS

- <http://tools.ietf.org/html/rfc6841>
- DPS for the Root Zone KSK Operator
  - <https://www.iana.org/dnssec/>
- Also review published DPS documents from TLDs who have already deployed DNSSEC



# DPS

- .SE's DNSSEC Practice Statement
  - [www.iis.se/docs/se-dnssec-dps-eng.pdf](http://www.iis.se/docs/se-dnssec-dps-eng.pdf)
- .CL's DNSSEC Practice Statement
  - <http://www.nic.cl/dnssec/en/dps.html>
- .NET DNSSEC Practice Statement
  - <http://www.verisigninc.com/assets/20100925-NET+DPS-FINAL.pdf>