

DNSSEC

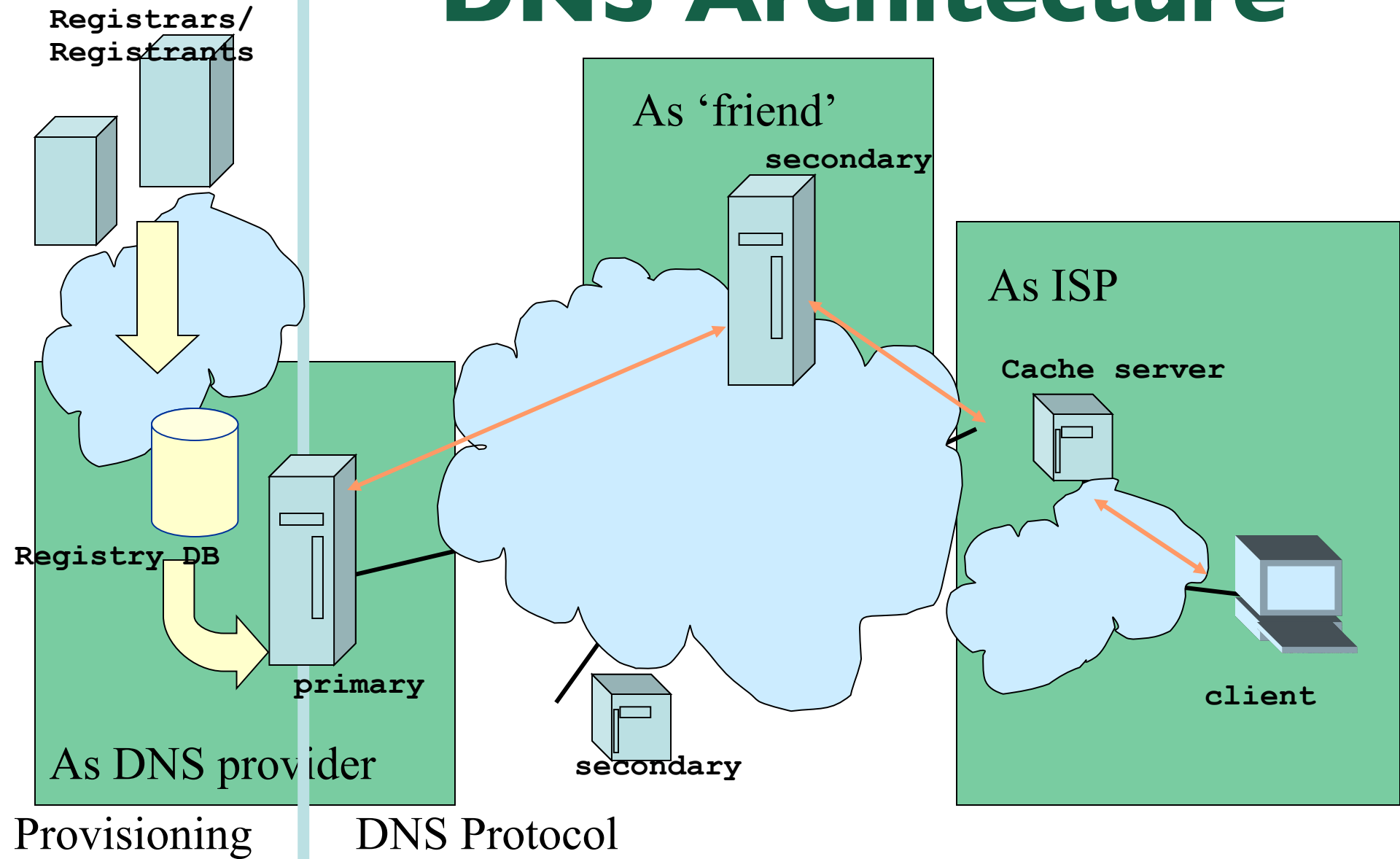
Part1: DNSSEC: Why and How

DNSSEC Tutorial

AfriNIC-17
Khartoum, Nov 2012

aalain@afriNIC.net

DNS Architecture



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

The Problem

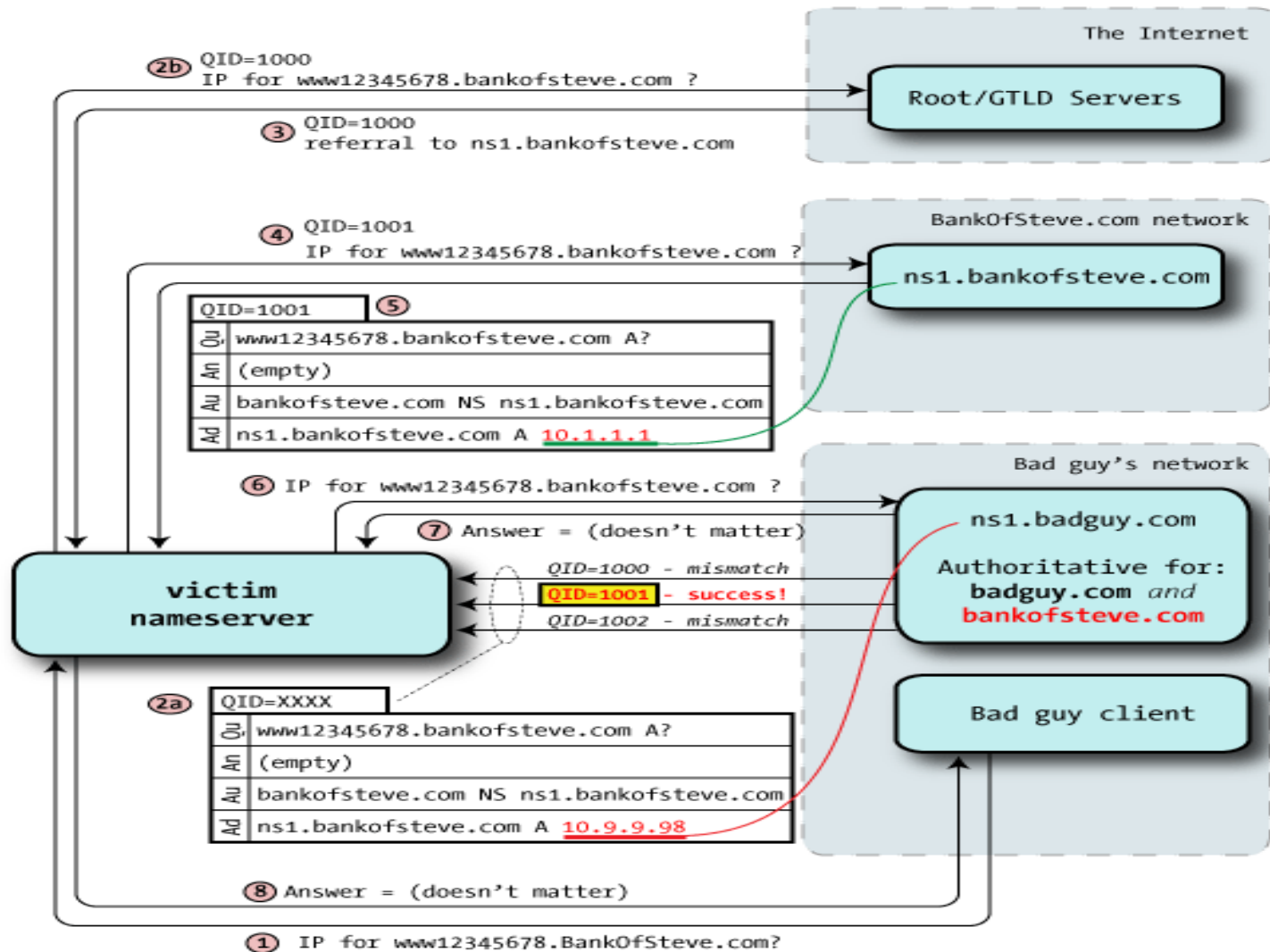
- DNS data published by the registry is being replaced on its path between the “server” and the “client”.
- This can happen in multiple places in the DNS architecture
 - DNS uses UDP, much easier to spoof
 - Some places are more vulnerable to attacks than others
 - Vulnerabilities in DNS software make 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

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

Kaminsky attack



Kaminsky attack (con't)

Stay Updated | [Metasploit Blog](#) | [Website Feedback](#)

[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 >`

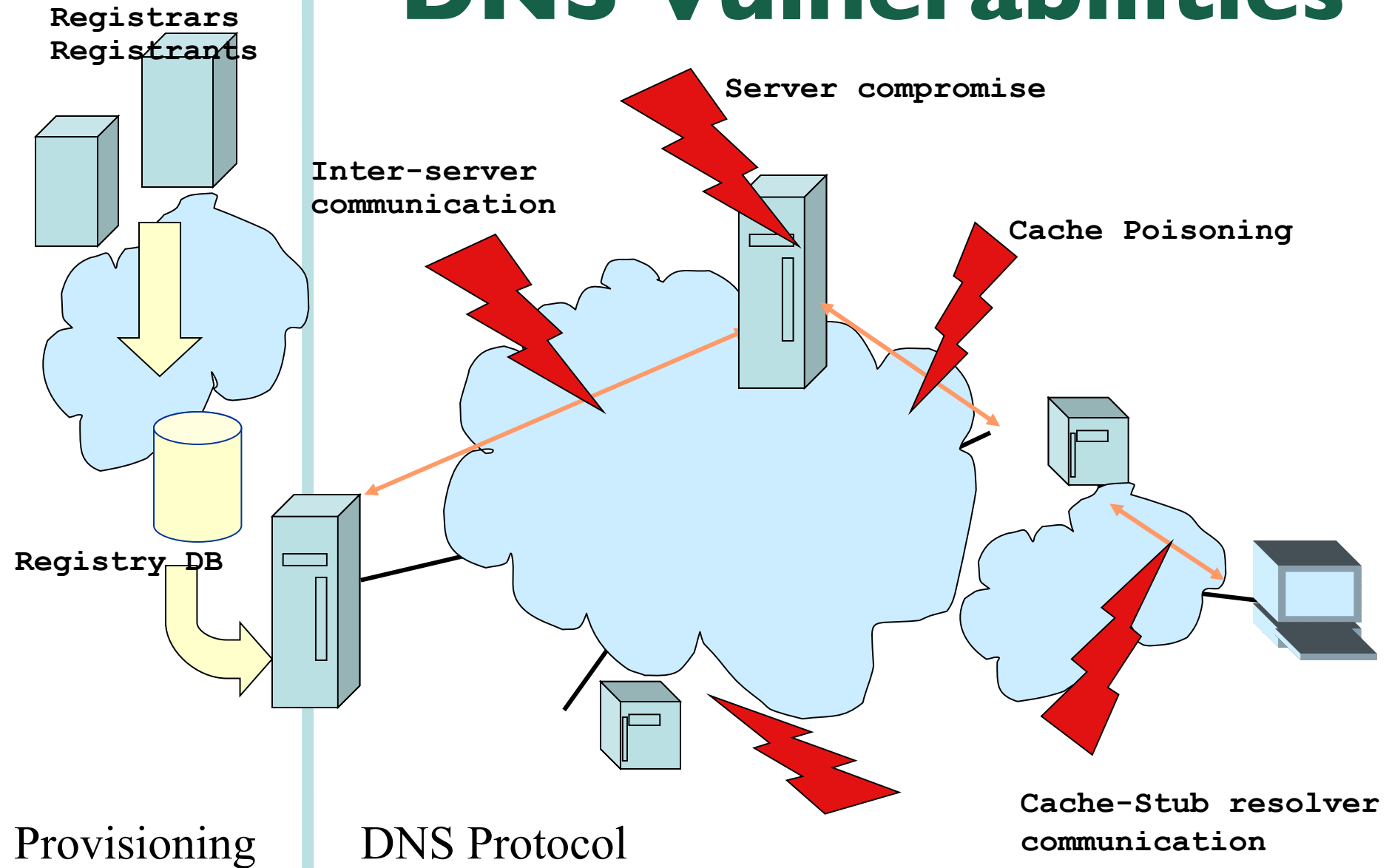
Vulnerability References

[CVE-2008-1447](#)
[OSVDB-46776](#)
[US-CERT-VU-800113](#)
<http://www.caughtq.org/exploits/CAU-EX-2008-0003.txt>

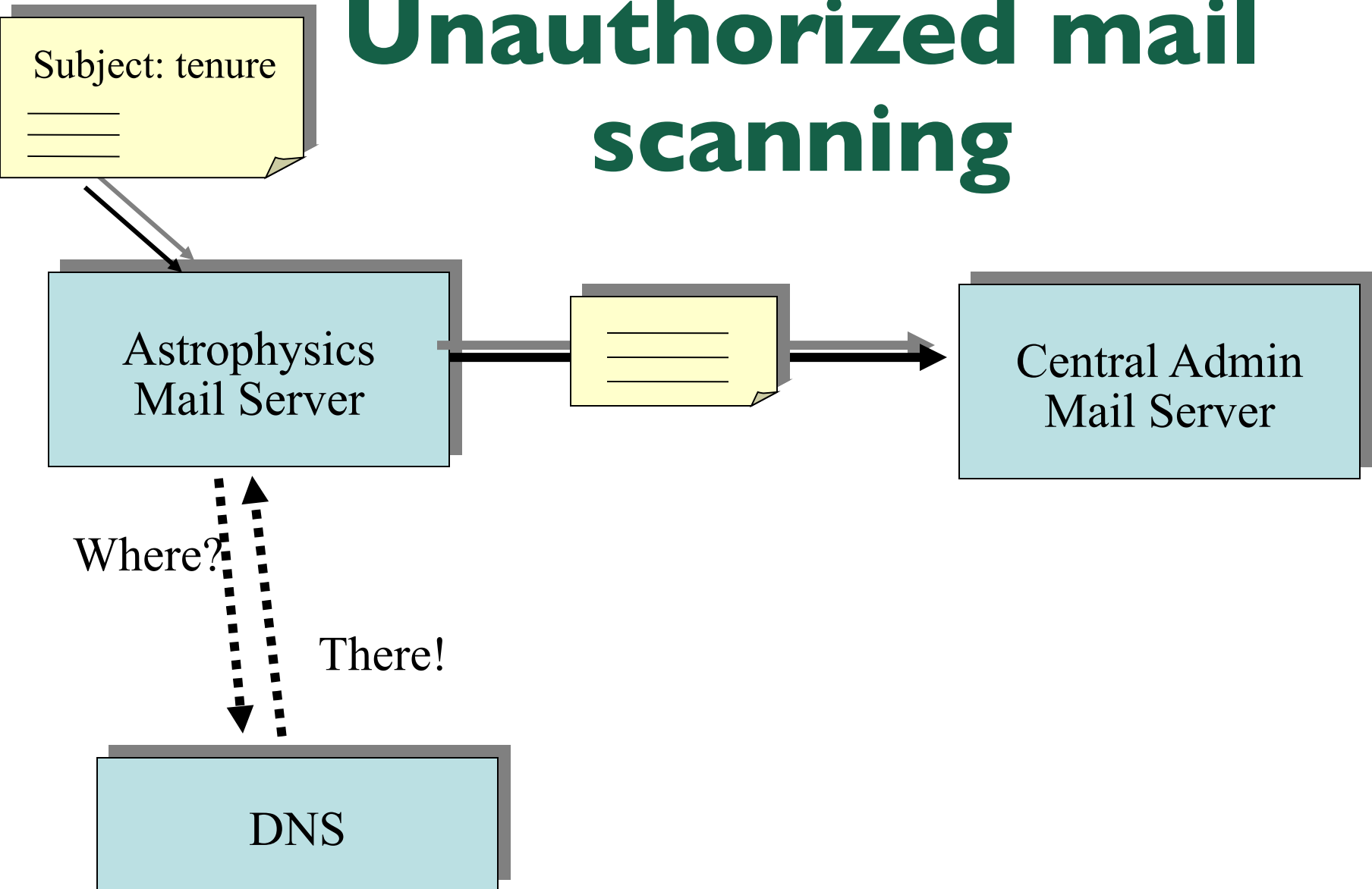
GET METASPLOIT FOR
PENETRATION
TESTING

FREE DOWNLOAD

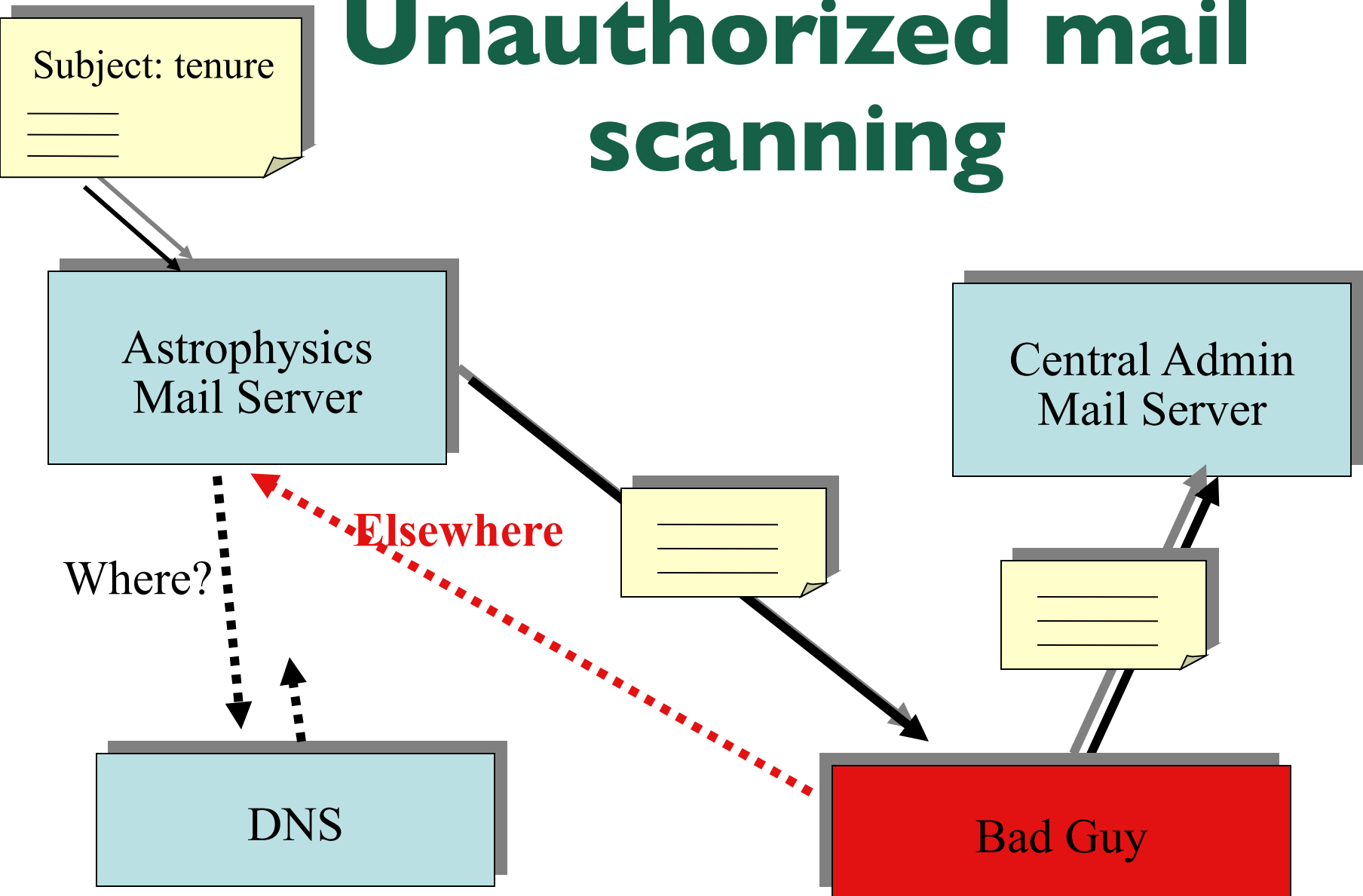
DNS Vulnerabilities



Example: Unauthorized mail scanning



Example: Unauthorized mail scanning



Where Does DNSSEC Come In?

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

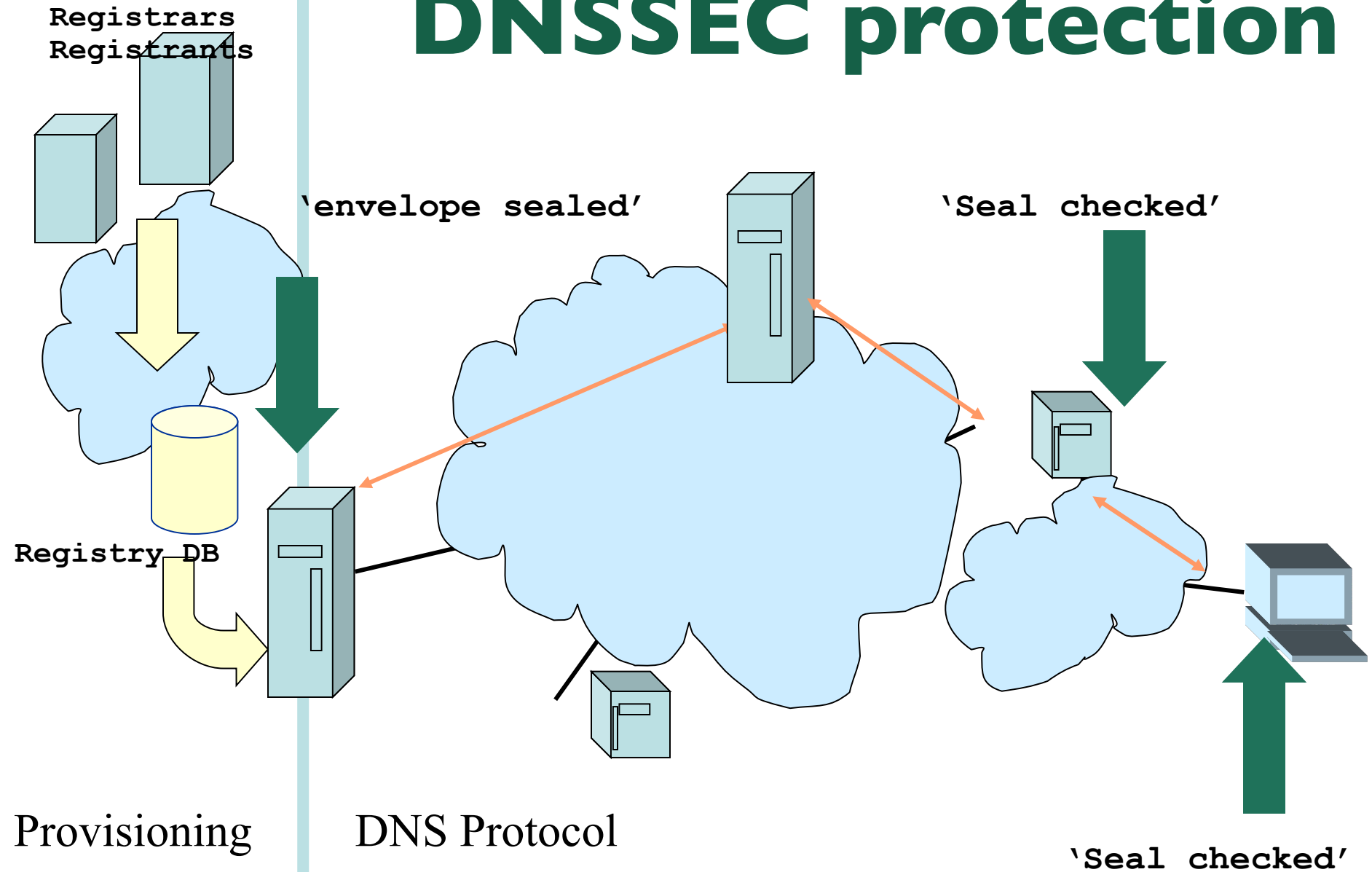
Authenticity and Integrity

- 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 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

DNSSEC protection



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

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 article: “Is Hierarchical Public-Key Certification the Next Target for Hackers?”

More benefits?

- With reasonable confidence perform opportunistic key exchanges
 - SSHFP, IPSECKEY X509 CERTS 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

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

http://threatpost.com/en_us/blogs/attackers-obtain-valid-cert-google-domains-mozilla-moves-revoke-it-082911 Reader Google

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 Google+ 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.

Editors Pick: Security and privacy experts began discussing the problem Monday

Go to "http://threatpost.com/en_us/blogs/attackers-obtain-valid-cert-google-domains-mozilla-moves-revoke-it-082911"

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

▶ Watch the animation now

Attacks against PKI(cont.)

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

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

Microsoft Revokes Trust in Five D... Capture a Screen Shot with Mac OS X

threatpost Monday, March 5th, 2012

The Kaspersky Lab Security News Service

Google Custom Search Search

Newsletter Sign-up

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

Twitter Facebook Reddit + Share Facebook Like 5 +1 0

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

A signed zone

[...]

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.pVlziETr5b3RjBR86rHTdgrJVEkL9QfHoUoR3mepL5wGIH8leJpeZQNjQPZM/AMzcEtiDmli2RXvpYLxTdBpdg
==)

[....]

trstech.net. 86400 **DNSKEY** 257 3 5
(AwEAAZrwNevGbMaT+yW9K+XILk6WqN3F1heks/tfUCjAVWLKYHKtB5+2GdCC7QW4MA3dwAKbpqv+4NSg/6yLwQz
BnF6gSRW3PhzIR53u8FdGF3yuYzTOd8HSL04otKZfmXAWnDSJfLY0WkZyycxB+tMWUWqEYWMhC5aZuTL7kHJndiz
3) ; key id = 36472

[.....]

trstech.net. 86400 **RRSIG** DNSKEY 5 2 86400 20061227191027 (20061127191027 33888 trstech.net.
J82iBTiEZOoheOMigH52SLtltXHij9jT12RlepZr9+EAeW/24wjJqvkcWLRN1DFYXTbK1V24F9NzkUh5TfeFw==)

[...]

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+FGO2Yr5fwOu3/uXyW/Ub4M6YobJNkhhtWW835Ff2qmZrpraFLp5ZNAK200M901uY7XI20O8nvRDv8XXb9Q==)

[...]

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
 - Parents always delegate security to child
 - ... but it doesn't help to sign if your parent doesn't sign, or isn't signed itself...

Trust Anchors repositories

- Root is signed and receiving DS records from TLDs
 - www.root-dnssec.org
- Incremental deployment of DNSSEC with multiples islands
- Use of Trust Anchors
 - *A DNS resource record store that contains SEP keys for one or more zones.*

Trust Anchor Repositories...

DLV

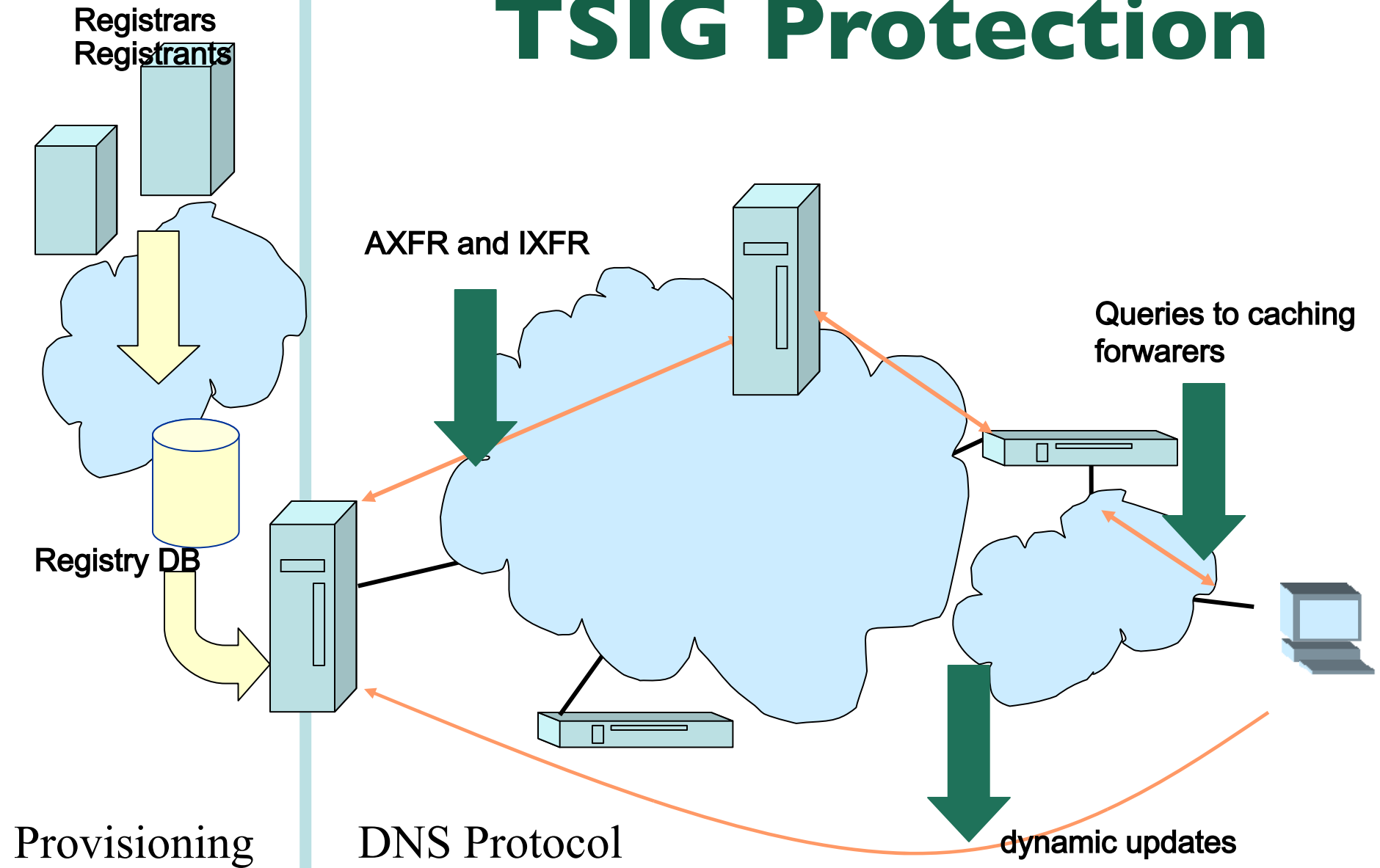
DLV: DNSSEC Lookaside Validation

- 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>

Other DNS security

- 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

TSIG Protection



Transaction Signature: TSIG

- TSIG (RFC 2845)
 - Authorising dynamic updates and zone transfers
 - Authentication of caching forwarders
 - Independent from other features of DNSSEC
- One-way hash function
 - DNS question or answer and timestamp
- Traffic signed with “shared secret” key
- Used in configuration, **NOT** in zone file

TSIG for Zone Transfers

- Generate secret
- Communicate secret
- Configure servers
- Test

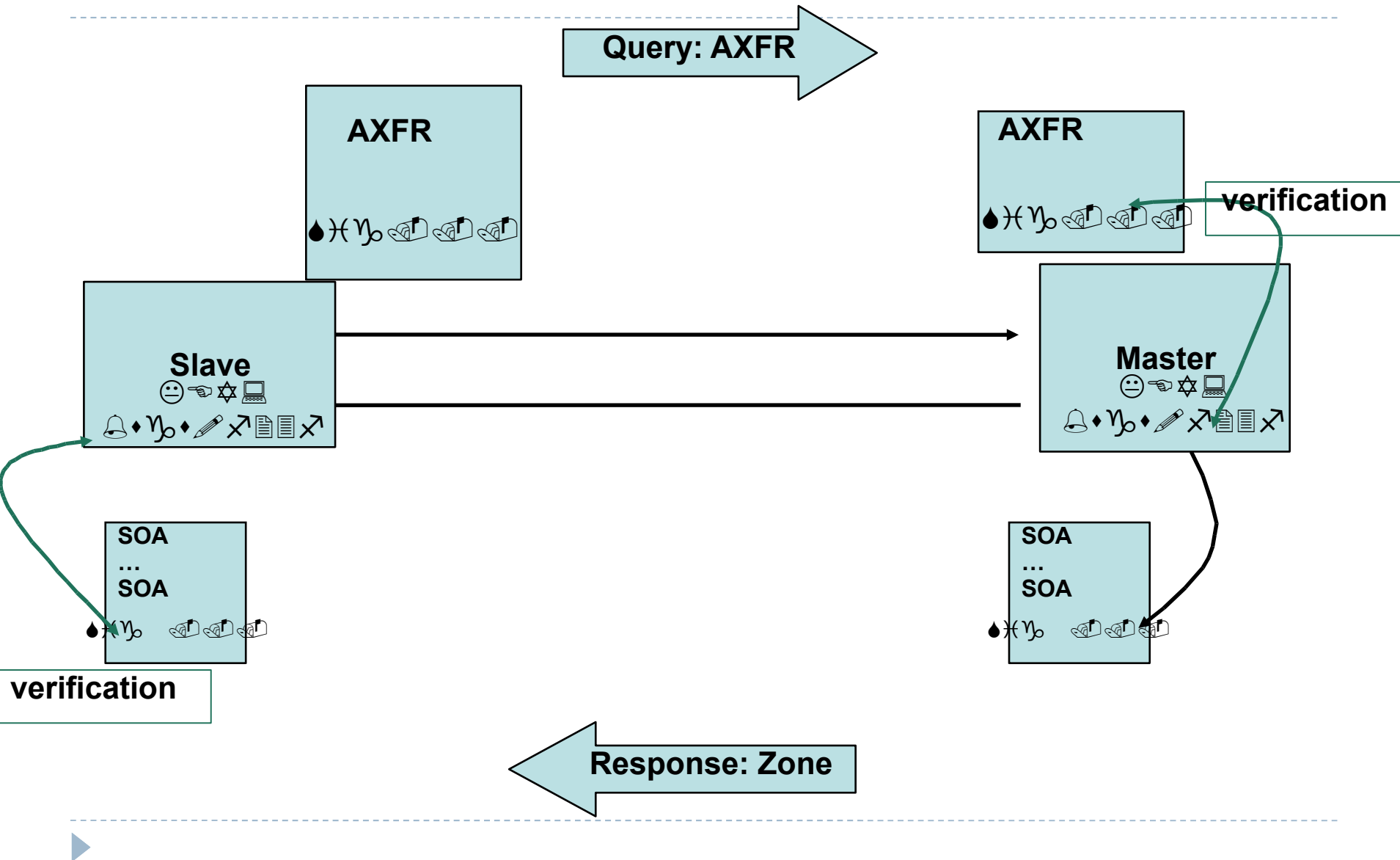
Importance of the Time Stamp

- TSIG/SIG(0) signs a complete DNS request / response with time stamp
 - To prevent replay attacks
 - Currently hardcoded at five minutes
- Operational problems when comparing times
 - Make sure your local time zone is properly defined
 - **date -u** will give UTC time, easy to compare between the two systems
 - Use NTP synchronisation!

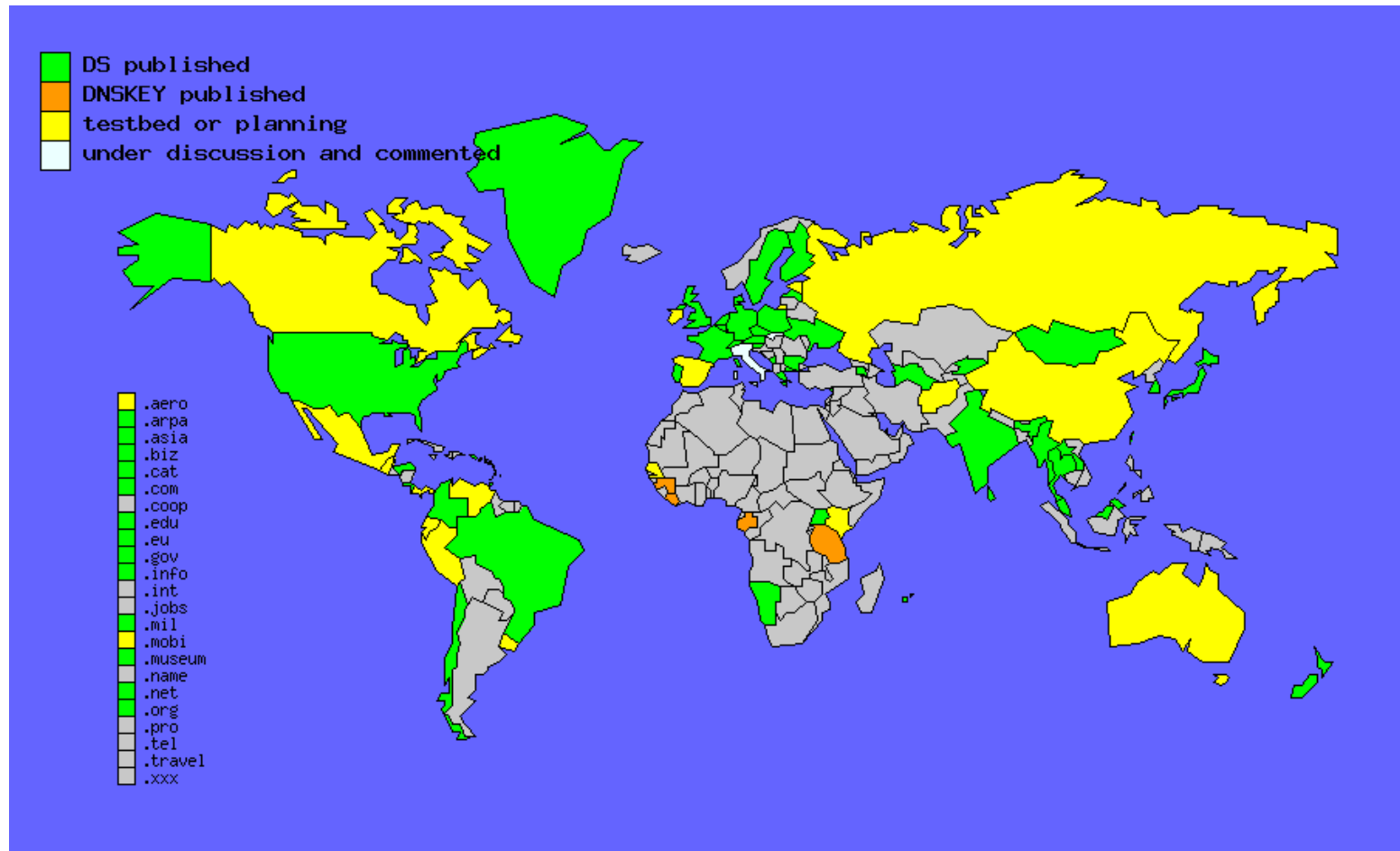
Authenticating Servers Using SIG(0)

- Alternatively, it is possible to use SIG(0)
 - Not yet widely used
 - Works well in dynamic update environment
- Public key algorithm
 - Authentication against a public key published in the DNS
- SIG(0) specified in RFC 2931

TSIG Example



DNSSEC Adoption



<http://www.ohmo.to/dnssec/maps/> seen today

Operator Guidance Documentation

NIST Special Publication 800-81	Recommendations of the National Institute of Science and Technology, Deployment Guide	NIST	http://csrc.nist.gov/publications/nistpubs/
RFC 4641	DNSSEC Operational Practices	IETF	http://www.ietf.org/rfc/rfc4641.txt
Step-by-Step guides	Guides for signed zone operation	SPARTA, Inc	http://www.dnssec-tools.org/resources/documentation.html
DNSSEC Howto	A tutorial in disguise	NLNet Labs	http://www.nlnetlabs.nl/dnssec_howto/

RFC4641bis <http://tools.ietf.org/wg/dnsop/draft-ietf-dnsop-rfc4641bis/>

Resources

www.dnssec-deployment.org

Includes monthly newsletter, DNSSEC This Month

DNSSEC Deployment Mailing list

dnssec-deployment-subscribe@shinkuro.com

www.dnssec-tools.org/

www.dnssec.net/

www.isc.org

Internet Systems Consortium – BIND, DLV

www.nlnetlabs.nl

NLnet Labs – NSD, Unbound

www.opendnssec.org

DNS visualization tool (<http://dnsviz.net/>)

Questions?

ASK