DNSSEC Briefing for GAC and ccNSO

ICANN

Steve Crocker
Chair, SSAC

October 30, 2007

Los Angeles, CA, USA

Topics

- Infrastructure Security Taxonomy
- DNSSEC walk through
- IANA Progress -- Richard Lamb
- Issues and Noise
- Discussion of Signing the Root

- With help from Russ Mundy, Olaf Kolkman, Patrik Fältström

Internet Infrastructure Security Threats

ICANN

Type of Attack	Impact	Fixes
Denial of Service Attacks	!!!	??
DNS Hijacking	!!	+++
Address & Route Hijacking	!	-

Internet Infrastructure Security Threats

Denial of Service Attacks	!!!	??

Biggest threat on the net. No good solutions: Massive capacity and quick reaction to attacks.

Systematic changes and law enforcement

Different briefing. Long term problem.

Internet Infrastructure Security Threats

DNS Hijacking	!!	+++

Serious threat. Easy to steal passwords, etc.

Good news: Solid technical solution

This is today's business

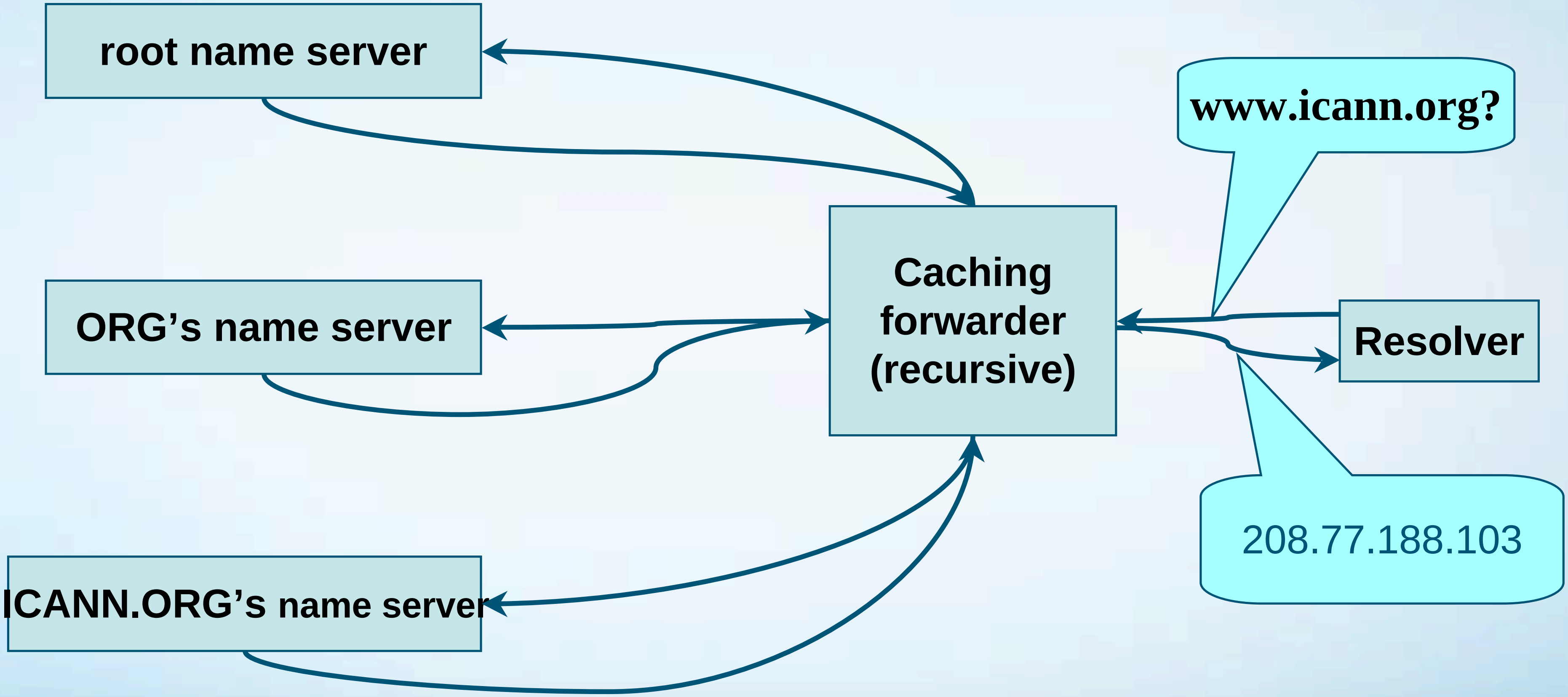
Internet Infrastructure Security Threats

Address & Route Hijacking	!	-

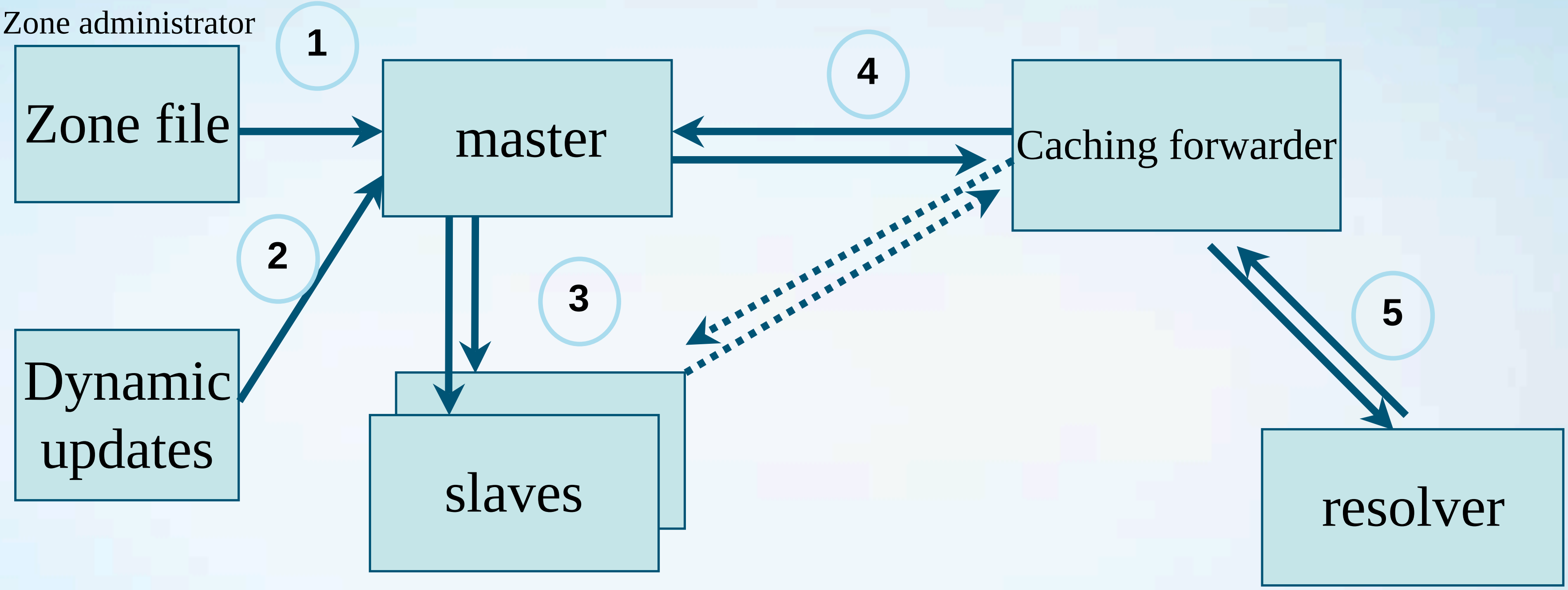
Potential threat.

Solvable, but work is still in progress

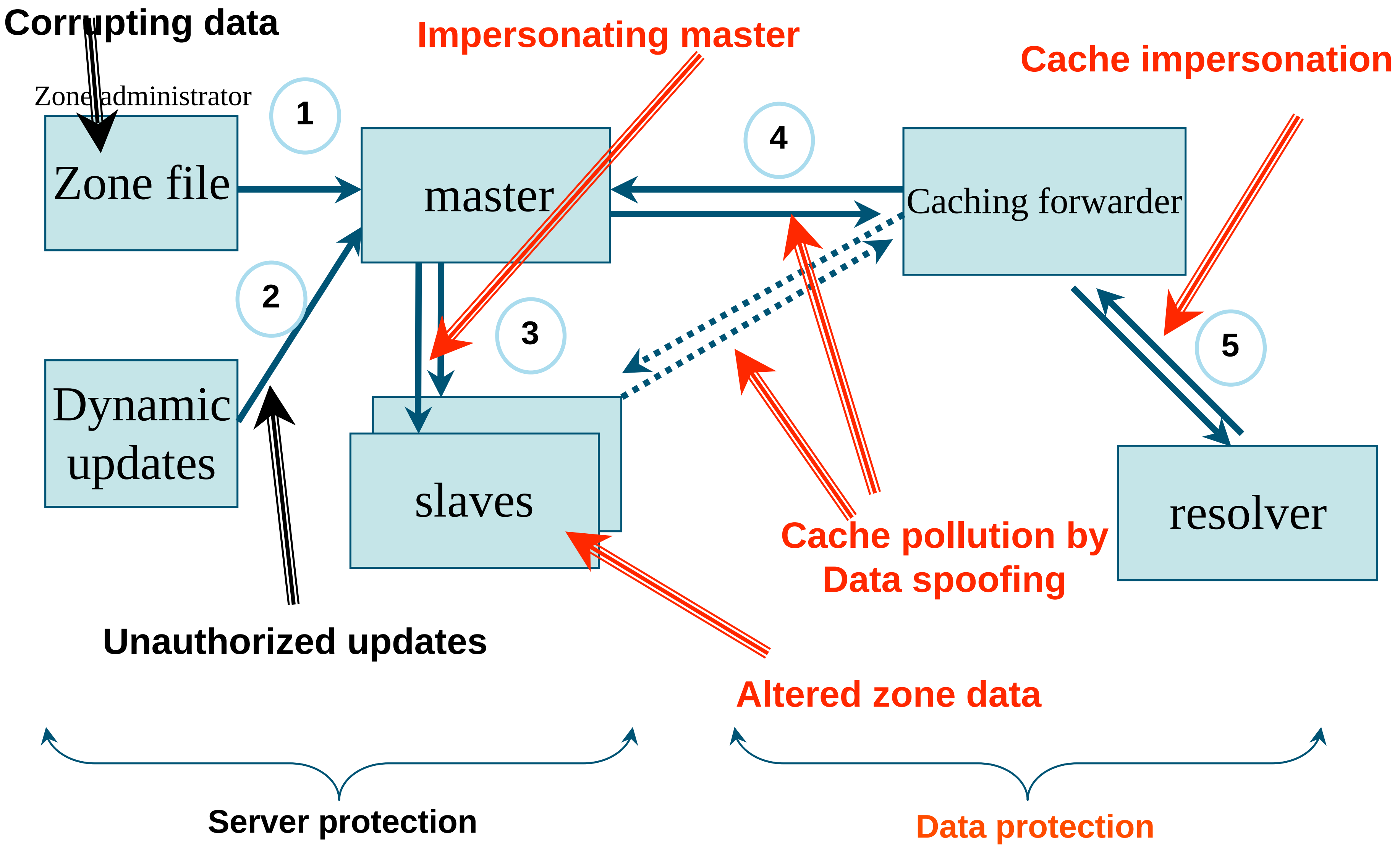
What is WWW.ICANN.ORG's address?



DNS: Data Flow



DNS Vulnerabilities



How bad can it get?

- In wireless environments, it’s easy to substitute DNS responses.
- Redirect to a false site
  - Steal passwords
- Redirect to a man-in-the-middle site
  - See and copy an entire session
  - Web, email, IM, etc.

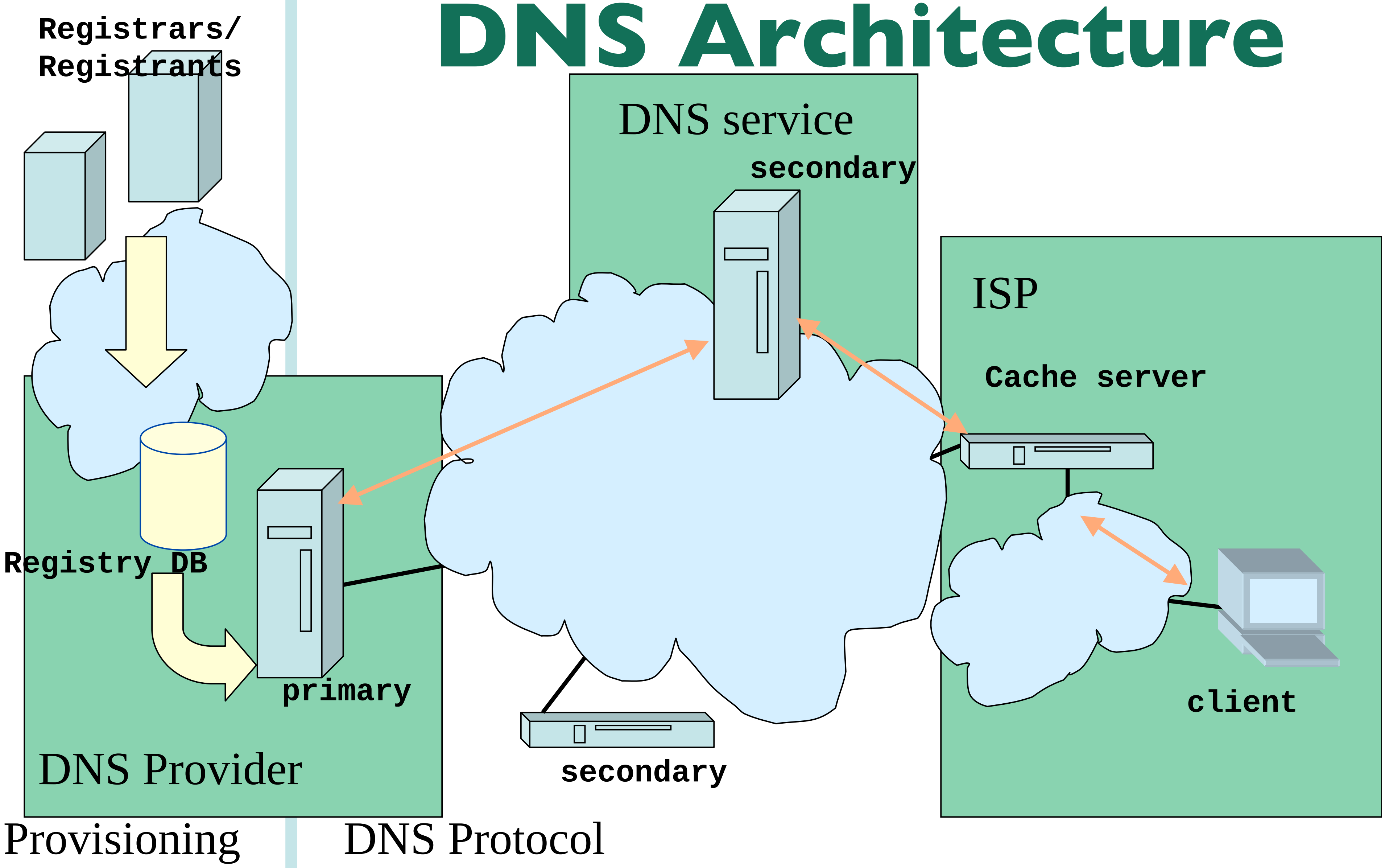
Why DNSSEC

- 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

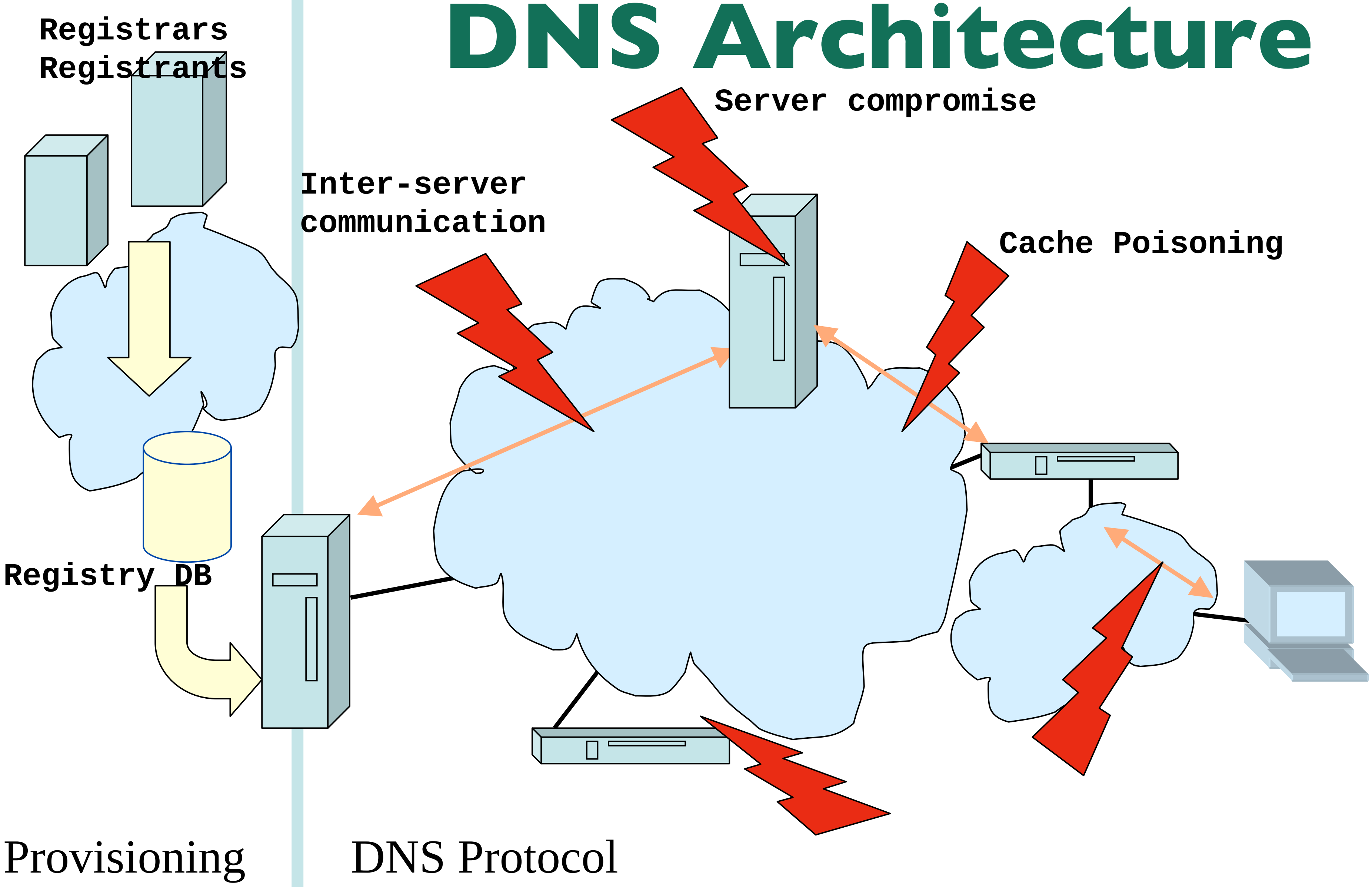
The Problem

- 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)

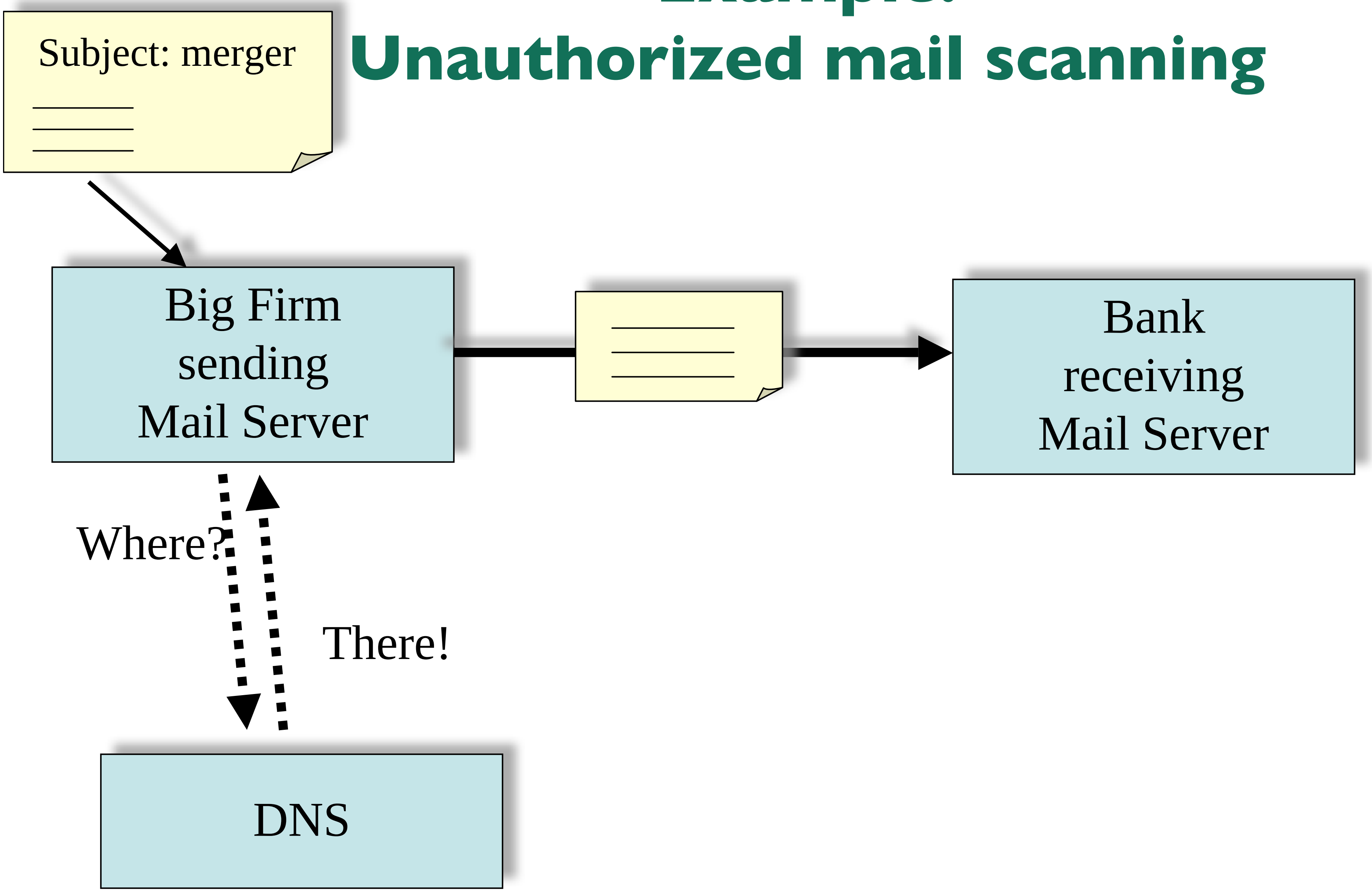
DNS Architecture



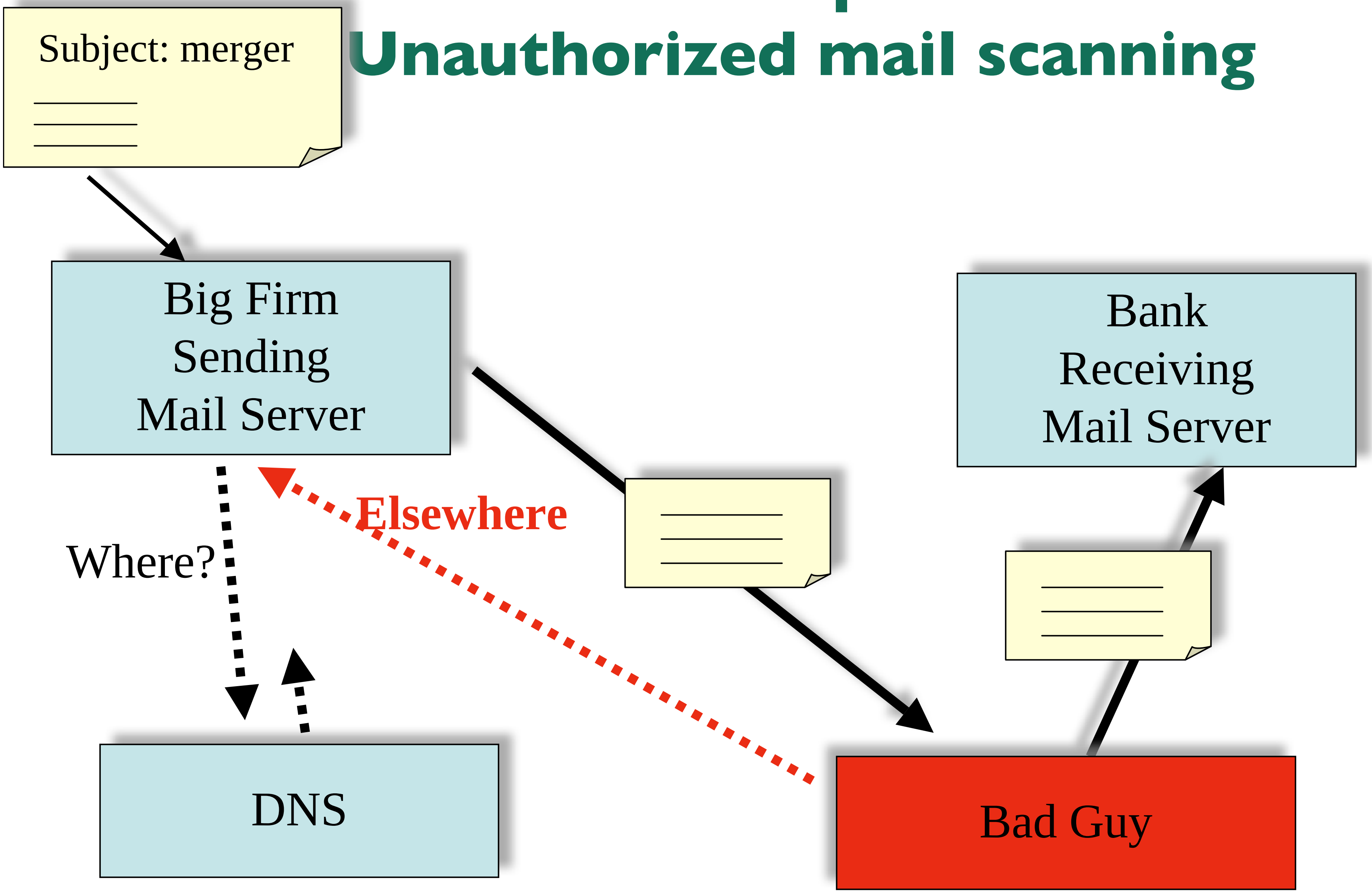
DNS Architecture



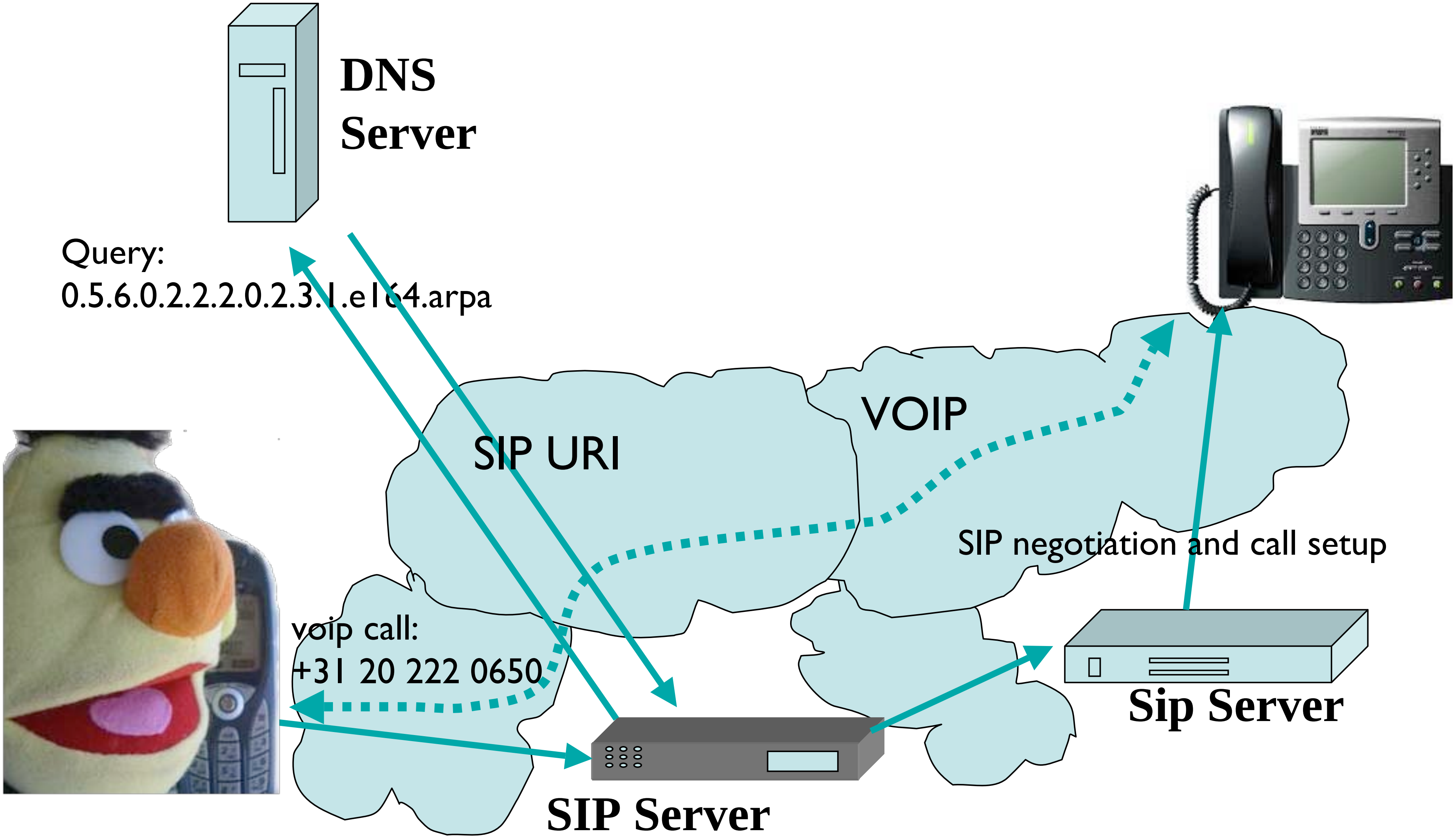
Example: Unauthorized mail scanning



Example: Unauthorized mail scanning

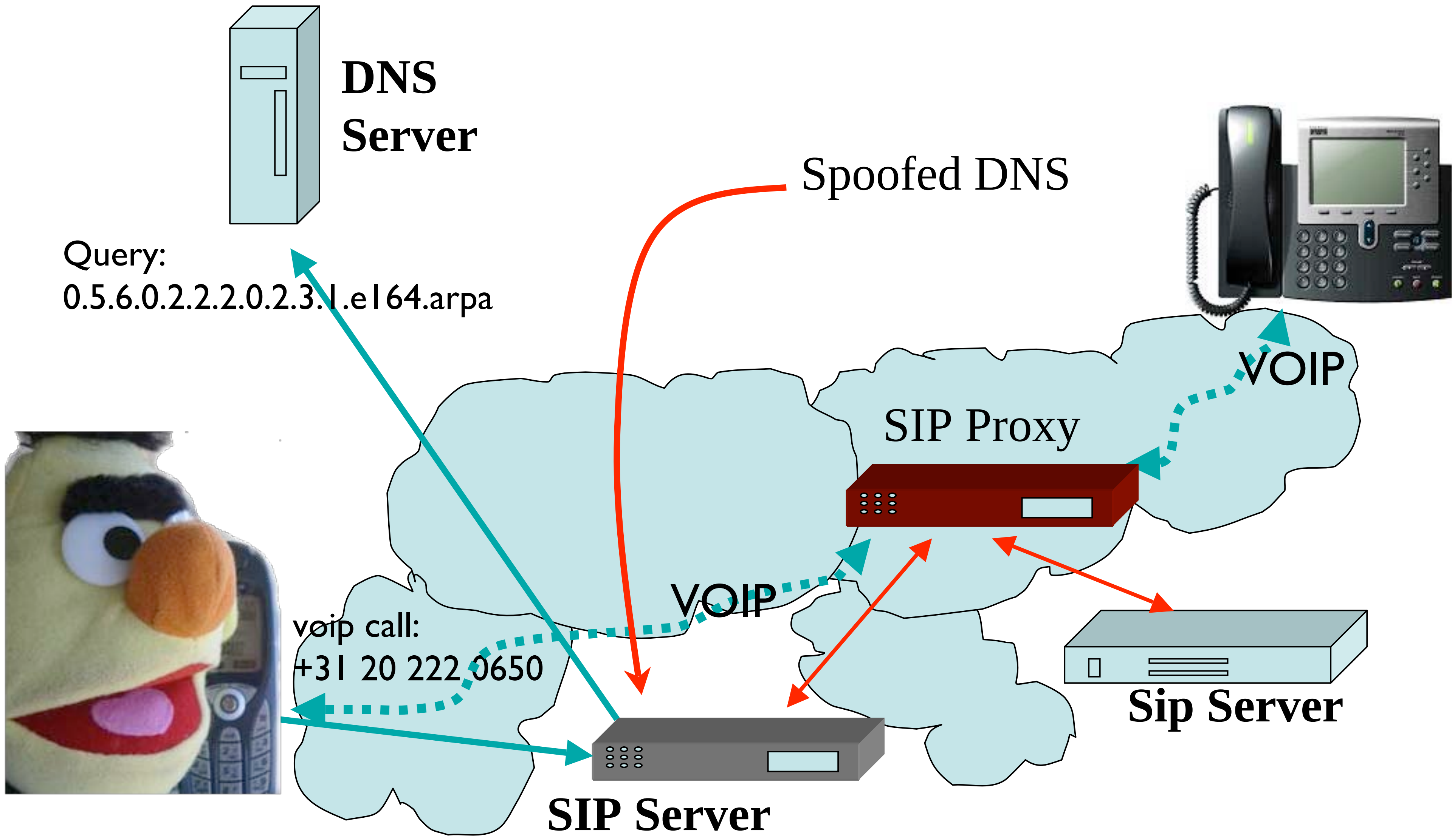


voip2voip as an example



Slide courtesy: Patrik Fältström

voip2voip as an example



Slide courtesy: Patrik Fältström

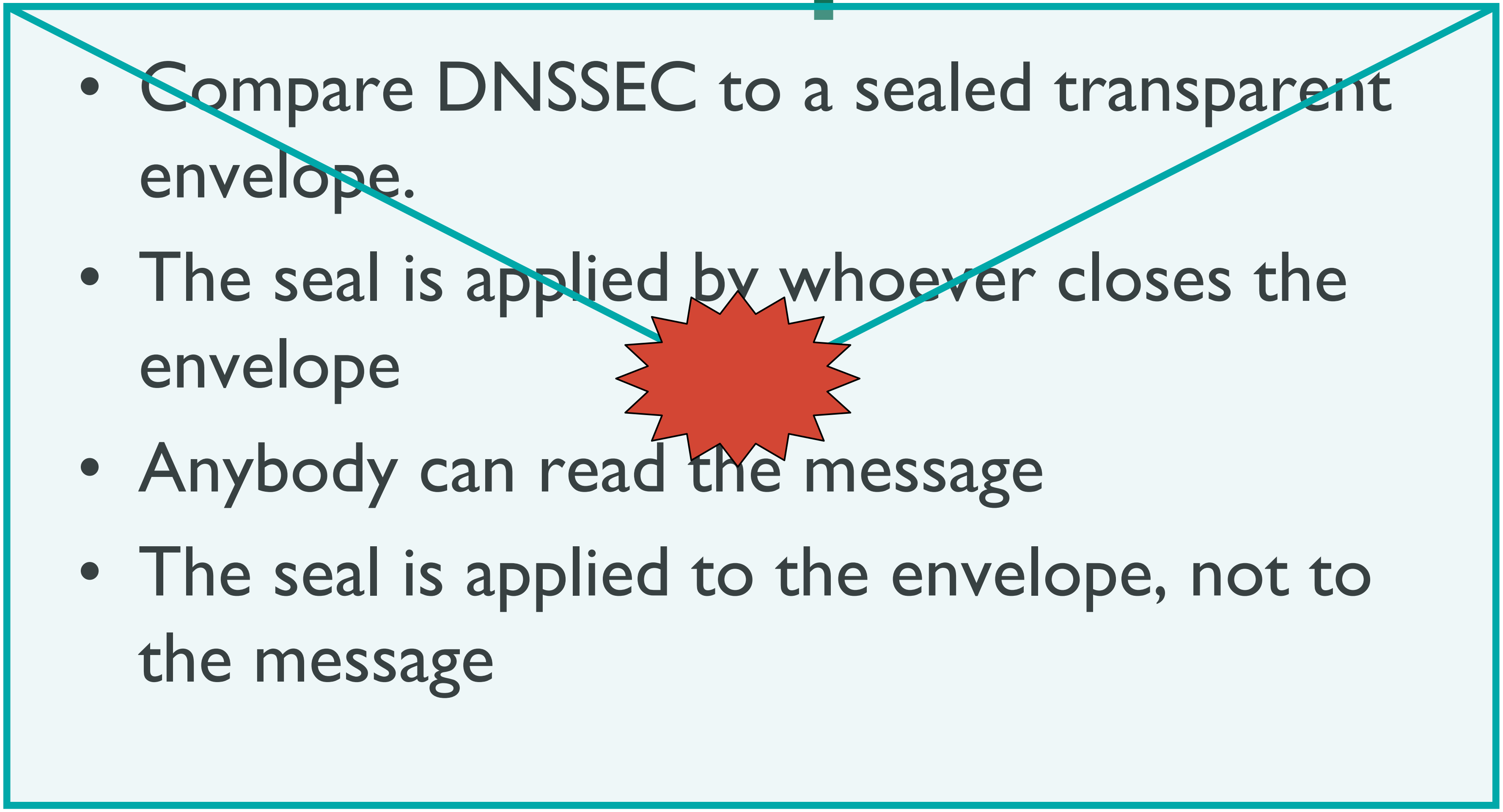
Targets; Where DNS and economics meet?

- SPF, DKIM, DomainKey and family
  - Technologies that use the DNS to mitigate spam and phishing: $$$ value for the black hats
- Stock tickers, RSS feeds
  - Usually no source authentication but supplying false stock information via a stock ticker and via a news feed can have $$$ value
- ENUM
  - Using telephone numbers as identifyers to lookup services in the DNS
  - Both in user-enum and infrastructure-enum

Where Does DNSSEC Come In?

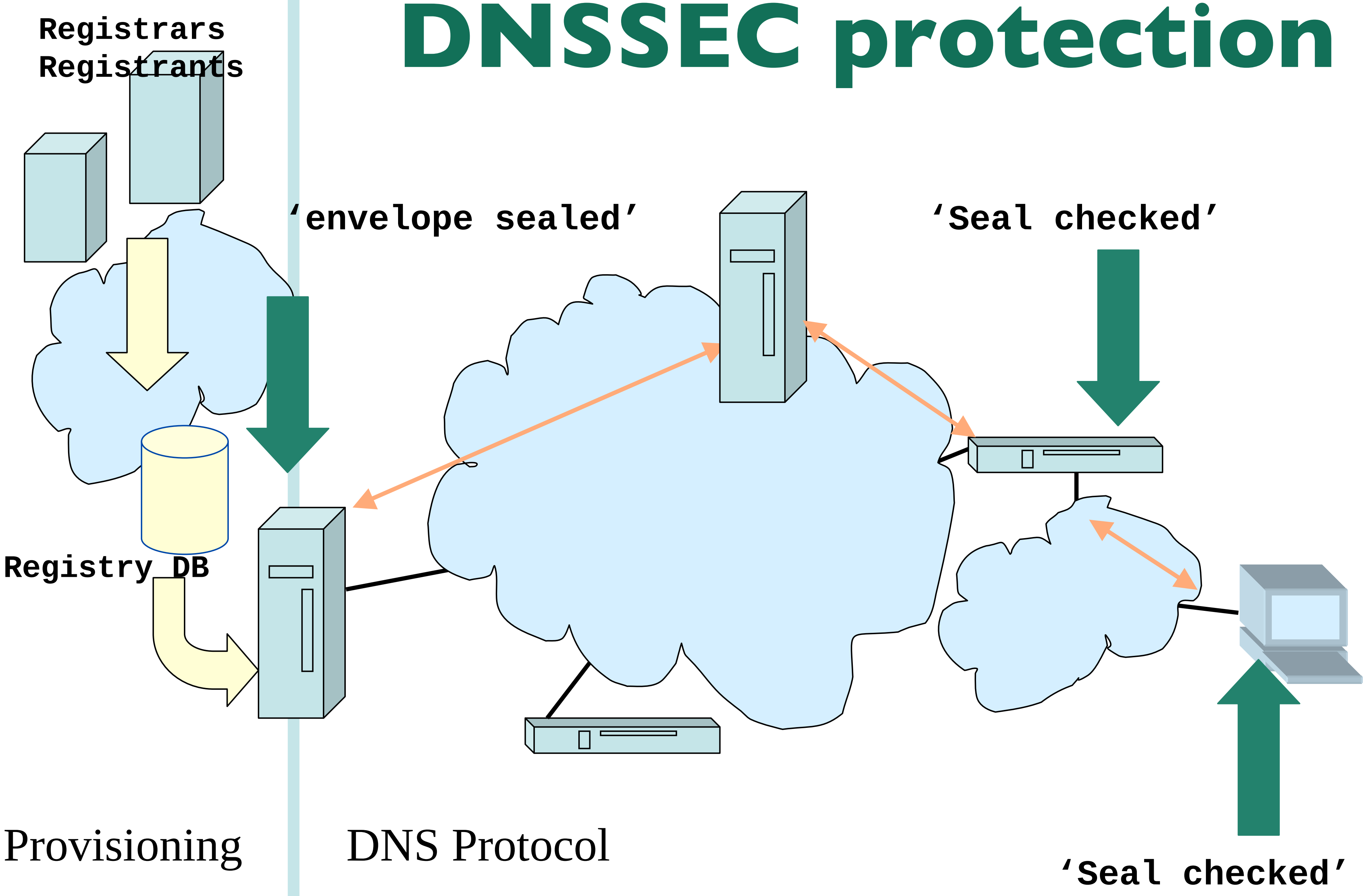
- DNSSEC secures the name to address mapping
  - Transport and Application security are just other layers.

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

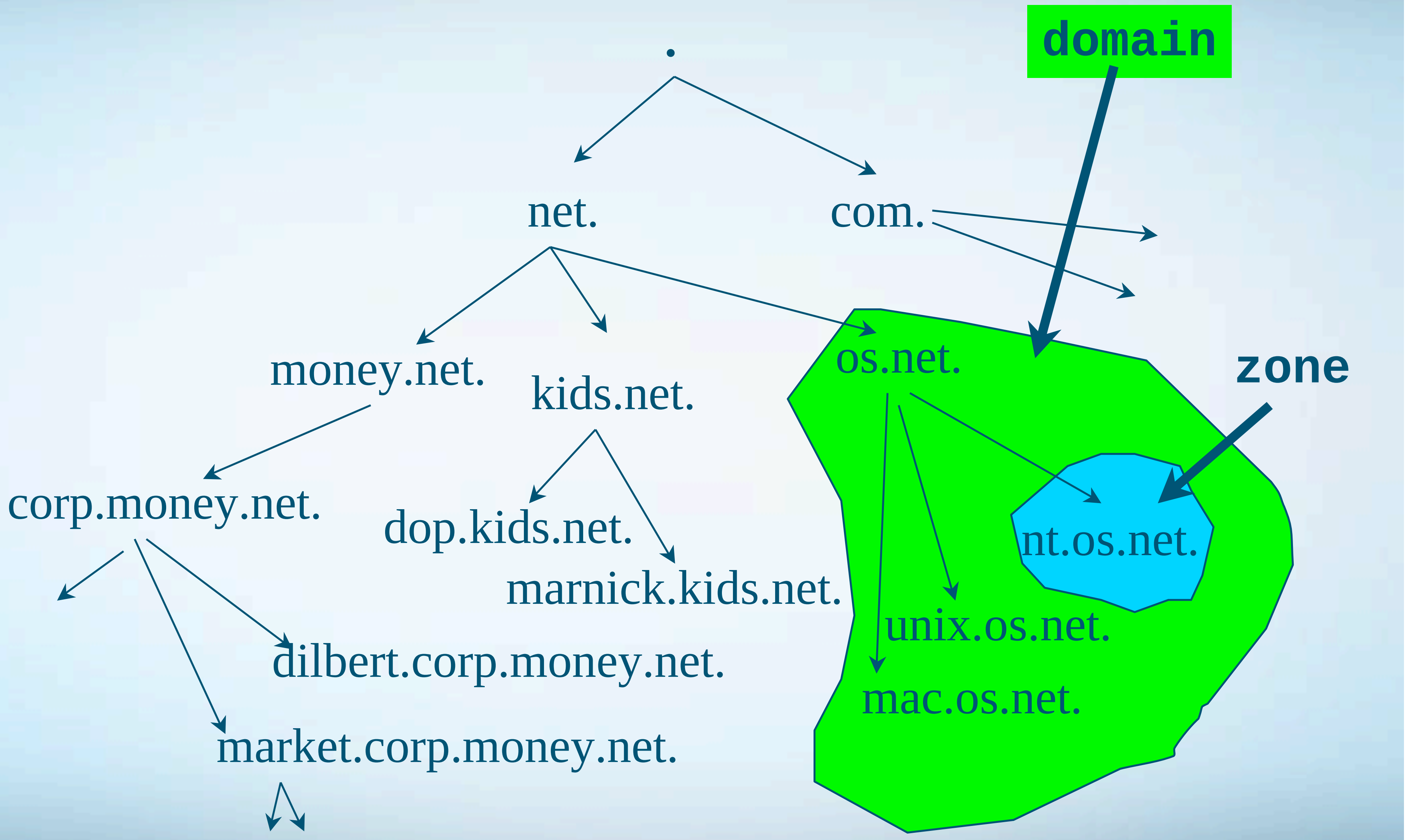
DNSSEC protection



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

DNS Content Structure



Deployment Status

- Signed: Sweden (.SE), Bulgaria (.BG), Puerto Rico (.PR), Brazil (.BR)
  - RIPE’s portion of in-addr.arpa too
- Under Development: Japan (.JP), Korea (.KR), Mexico (.MX), Taiwan (.TW), United Kingdon (.UK)
- .MIL, .GOV, .EDU, .ORG all moving forward
- .ARPA almost ready; .INT too

DNSSEC @ IANA
Richard Lamb

2007 ICANN Meeting Los Angeles

SSAC Briefing for GAC and ccTLD Operators

Thanks to Many!!

- IANA's design is built on the trailblazing work by .SE. Without the generous help from Jakob Schlyter and others at .SE, I would still be lost.
- Thanks to nlnetlabs.nl, Olaf, and others for the INVALUABLE “DNSSEC HowTo” and RFC4641 (DNSSEC Operational Practices) documents...
- ...and to Steve Crocker's dnssec-deployment.org initiative and the President's IANA Consultation Committee for crucial guidance.

Targets

- **.arpa** infrastructure (formal request from IAB)
  - **in-addr.arpa** reverse mapping (e.g. 18.62.0.6 → 6.0.62.18.in-addr.arpa → eddie.mit.edu)
  - **ip6.arpa** reverse mapping
  - **urn.arpa** for dynamic discovery of URN addressing schemes
  - **uri.arpa** for dynamic discovery of URI addressing schemes
  - **iris.arpa** for use in CRISP

- **.int** international organizations (e.g. itso.int)

- Experimental root **“.”**

Status

- **.arpa** deployment ready but we have determined that a risk-analysis is necessary before moving to production
  - production zone must be secure and stable

- **.int** ready to go but waiting for policy

- root is outside of our control but we have a candidate implementation for testing purposes

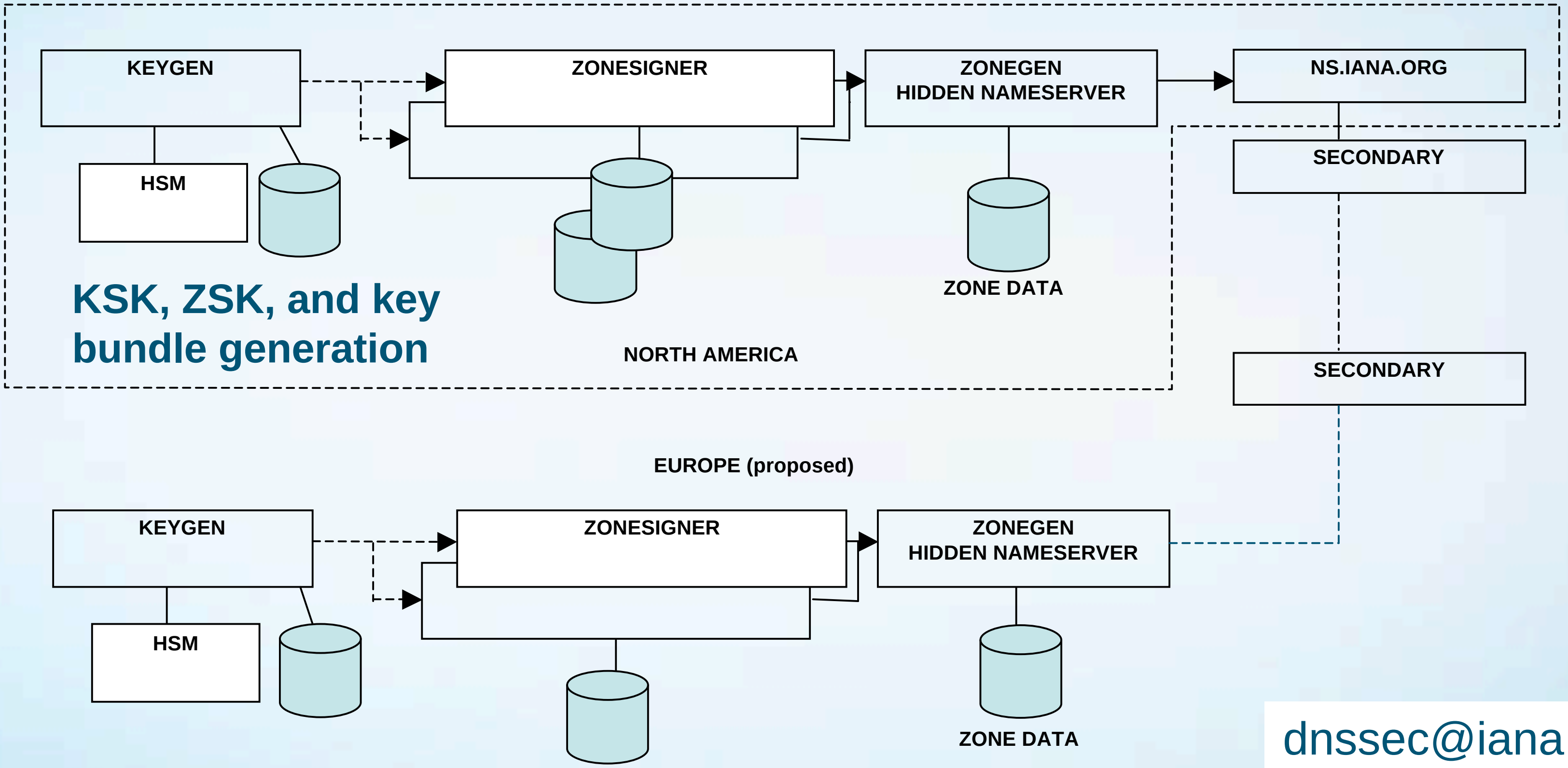
Design Goals

- Security
  - it must look and be secure for people to trust it
- Reliability and Maintainability
  - if its not easy, it will fail
  - if there is a problem, no one will use it
- Openness
  - Publish design and procedures
  - All software and modifications will be available as open source

Security – strong procedures and hardware

- Keys are long (1024/2048 bits) and changed regularly (monthly/yearly)
- Key generation responsibilities split among multiple people and requiring at least two (2) people to perform
- KSK can not be accessed in unencrypted form
- Encryption keys split among multiple people
- Key generation procedures are simple and logged

System Diagram



KSK, ZSK, and key bundle generation

dnssec@iana

Hardware

- 4x Dell 1RU 1950 commodity servers
- 1x AEP Keyper Pro (FIPS 140-2 Level 4) external Hardware Security Module (HSM)
- 1x KVM console
- Smart cards, Flash drive
- Locked rack within ICANN cage at secure colo facility

HSM – hardware security module

- To protect against internal as well as external attacks, KSK operations (generation, signing, backup) for critical zones are performed inside the HSM.
- Incorporated HSM by modifying BIND tools for native PKCS11 support
- HSM keys can only be backed up in encrypted form using and internal key
- Other unencrypted key material (e.g. ZSK) is also encrypted for back up using the HSM
- Only another HSM with the same internal HSM key can decrypt this material
- Internal HSM key backed up on N of M smartcards

Reliability

- Redundancy
  - Two (2) signing machines operating in parallel per site
  - Proposed mirror site
  - Multiple people trained to perform key generation procedures
- Simplicity
  - Automation to the maximum extent possible
  - Only two scripts (signall and keyall) to handle signing and key generation
- Testing – internal and external

Openness

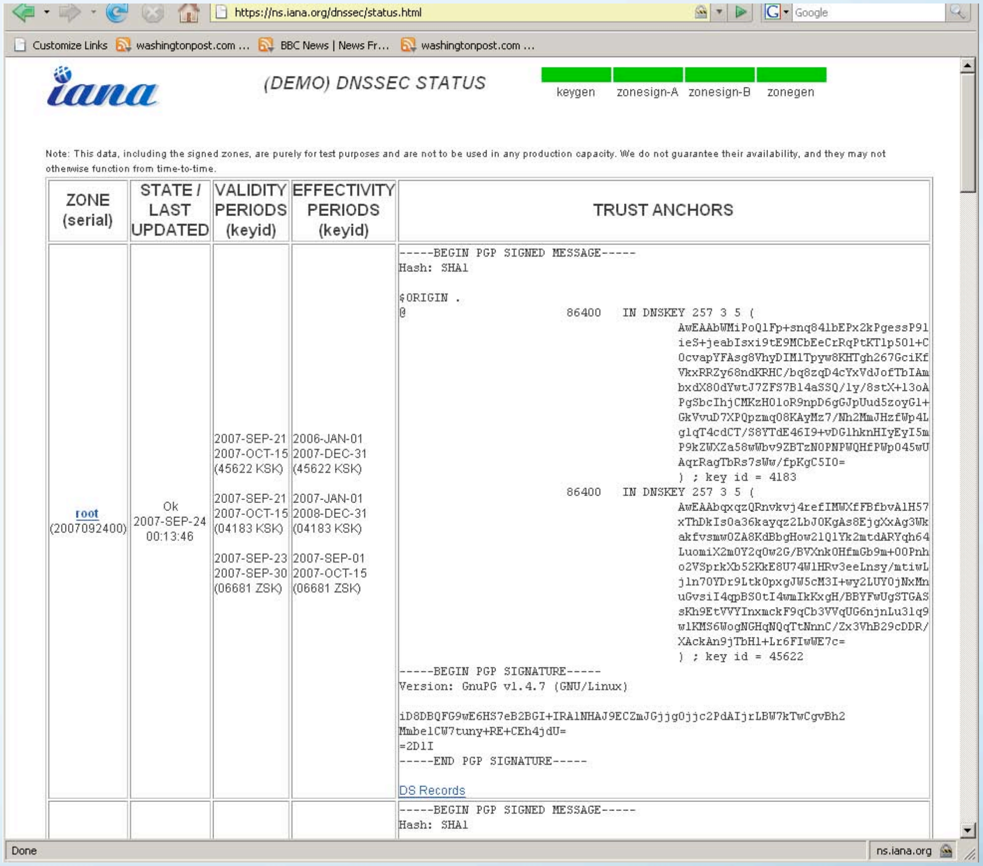
- Publication of design and procedures
- All software and modifications will be available as open source
- Use feedback from experts

DNSEC Status Page

https://ns.iana.org/dnssec/status.html

System status and publication of PGP signed trust anchors only on SSL secured site.

Domains: root, arpa, in-addr.arpa, uri.arpa, urn.arpa, iris.arpa, ip6.arpa, int



(DEMO) DNSSEC STATUS

🟩 keygen 🟩 zonesign-A 🟩 zonesign-B 🟩 zonegen

Note: This data, including the signed zones, are purely for test purposes and are not to be used in any production capacity. We do not guarantee their availability, and they may not otherwise function from time-to-time.

ZONE (serial)	STATE / LAST UPDATED	VALIDITY PERIODS (keyid)	EFFECTIVITY PERIODS (keyid)
root (2007092400)	Ok 2007-SEP-24 00:13:46	2007-SEP-21 2007-OCT-15 (45622 KSK) 2007-SEP-21 2007-OCT-15 (04183 KSK) 2007-SEP-23 2007-SEP-30 (06681 ZSK)	2006-JAN-01 2007-DEC-31 (45622 KSK) 2007-JAN-01 2008-DEC-31 (04183 KSK) 2007-SEP-01 2007-OCT-15 (06681 ZSK)

TRUST ANCHORS

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

$ORIGIN .
@                       86400   IN DNSKEY 257 3 5 (
                                        AwEAAbWMiPoQlFp+snq84lbEPx2kPgessP91
                                        ieS+jeabIsxi9tE9MCbEeCrRqPtKTlp50l+C
                                        OcvapYFAsg8VhyDIMlTpyw8KHTgh267GciKf
                                        VkxRRZy68ndKRHC/bq8zqD4cYxVdJofTbIAm
                                        bxdX80dYwtJ7ZFS7Bl4aSSQ/ly/8stX+l3oA
                                        PgSbcIhjCMKzH0loR9npD6gGJpUud5zoyGl+
                                        GkVvuD7XPQpzmq08KAyMz7/Nh2MmJHzfWp4L
                                        glqT4cdCT/S8YTdE46I9+vDGlhknHIyEyI5m
                                        P9kZWXZa58wWbv9ZBTzN0PNPWQHfPWp045wU
                                        AqrRagTbRs7sWw/fpKgC5IO=
                                        ) ; key id = 4183
                        86400   IN DNSKEY 257 3 5 (
                                        AwEAAbqxqzQRnvkvj4refIMWXfFBfbvAlH57
                                        xThDkIs0a36kayqz2LbJ0KgAs8EjgXxAg3Wk
                                        akfvsmw0ZA8KdBbgHow21QlYk2mtdARYqh64
                                        LuomiX2m0Y2q0w2G/BVXnk0HfmGb9m+00Pnh
                                        o2VSprkXb52KkE8U74WlHRv3eeLnsy/mtiwL
                                        jln70YDr9Ltk0pxgJW5cM3I+wy2LUY0jNxMn
                                        uGvsiI4qpBS0tI4wmIkKxgH/BBYFwUgSTGAS
                                        sKh9EtVVYInxmckF9qCb3VVqUG6njnLu3lq9
                                        wlKMS6WogNGHqNQqTtNnnC/Zx3VhB29cDDR/
                                        XAckAn9jTbHl+Lr6FIwWE7c=
                                        ) ; key id = 45622
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.7 (GNU/Linux)

iD8DBQFG9wE6HS7eB2BGI+IRAlNHAJ9ECZmJGjjg0jjc2PdAIjrLBW7kTwCgvBh2
MmbelCW7tuny+RE+CEh4jdU=
=2DlI
-----END PGP SIGNATURE-----
```

DS Records

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
```

Try it!

Try it! “dig +dnssec -t soa . @ns.iana.org”

Questions?

Issues and noise

- Performance
- Privacy
- Makes DDoS worse
- No market pressure
- Root isn’t signed

Performance

- On the server side
  - More memory is needed
  - More bandwidth is needed
  - CPU load is about the same

  No problem; there is a lot of excess capacity

- On the client side, not enough data yet, but shouldn't be a problem

Privacy

- Claim: A signed zone can be “walked” to learn its contents
- Modification (NSEC3) is designed and approved. Will be an RFC very soon.

Makes DDoS worse

- Claim: DNSSEC increases load on name servers, making them weaker against DDoS attacks
- Answer: Not really. Difference is small

- Claim: DNSSEC makes responses longer. Bigger impact of Amplified DDoS attacks.
- Answer: 4000 bytes is already big enough to hurt

No Market Pressure

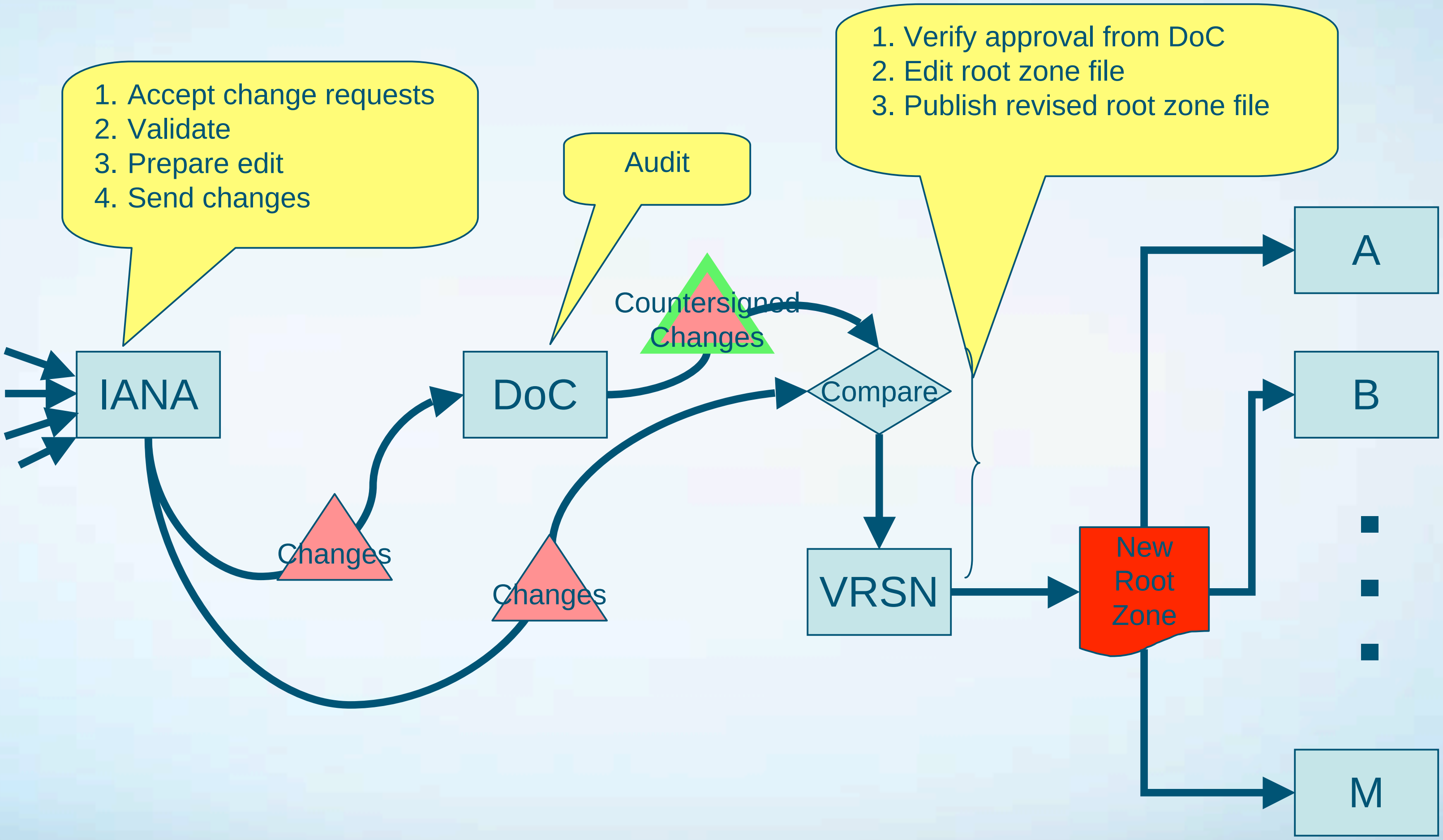
- Claim: My users aren’t asking for this? Why should I invest?
- It’s part of protecting the infrastructure. The standard of care is getting higher.

The Root isn’t Signed

- Claim: Why should my zone be signed if the root isn’t signed?
- Answer: Every zone should be signed. All will come together. The root has high political significance, but relatively small engineering impact.
  - Root has <300 children
  - Most TLDs have many, many more children

The Role of the Root Key

Root Zone Change Flow



1. Accept change requests
2. Validate
3. Prepare edit
4. Send changes

Audit

1. Verify approval from DoC
2. Edit root zone file
3. Publish revised root zone file

Content vs Signatures

- The content of the root zone is under firm control. Signing won't change process.
- Signature adds assurance.
- Signature does not control content.

But what if…?

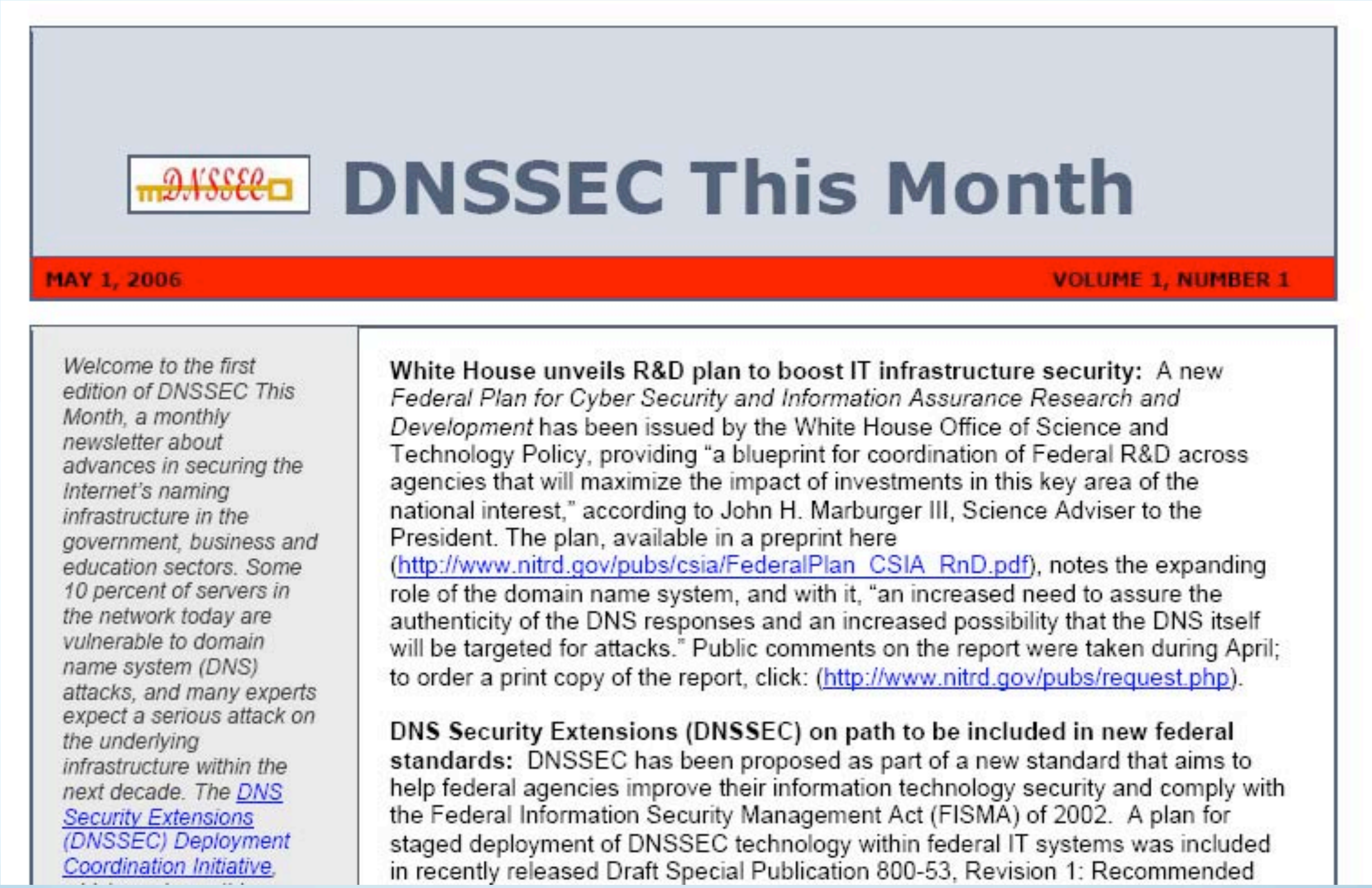
- What if the keyholder creates a false root zone?
- Well…
  - He'd have to get it to you
  - And he'd have to keep it out of sight of others

  - If he can do that with a signature, he can also do that today.

So why the fuss about the root key?

- Anything related to cryptography feels spooky.
- Signatures are not “encryption.” Nothing is hidden.
- The community needs a clean, simple, visible, well documented and well run system.

DNSSEC THIS MONTH
(http://www.dnssec-deployment.org)



DNSSEC This Month

MAY 1, 2006 VOLUME 1, NUMBER 1

Welcome to the first edition of DNSSEC This Month, a monthly newsletter about advances in securing the Internet's naming infrastructure in the government, business and education sectors. Some 10 percent of servers in the network today are vulnerable to domain name system (DNS) attacks, and many experts expect a serious attack on the underlying infrastructure within the next decade. The DNS Security Extensions (DNSSEC) Deployment Coordination Initiative,

White House unveils R&D plan to boost IT infrastructure security: A new *Federal Plan for Cyber Security and Information Assurance Research and Development* has been issued by the White House Office of Science and Technology Policy, providing "a blueprint for coordination of Federal R&D across agencies that will maximize the impact of investments in this key area of the national interest," according to John H. Marburger III, Science Adviser to the President. The plan, available in a preprint here (http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf), notes the expanding role of the domain name system, and with it, "an increased need to assure the authenticity of the DNS responses and an increased possibility that the DNS itself will be targeted for attacks." Public comments on the report were taken during April; to order a print copy of the report, click: (http://www.nitrd.gov/pubs/request.php).

DNS Security Extensions (DNSSEC) on path to be included in new federal standards: DNSSEC has been proposed as part of a new standard that aims to help federal agencies improve their information technology security and comply with the Federal Information Security Management Act (FISMA) of 2002. A plan for staged deployment of DNSSEC technology within federal IT systems was included in recently released Draft Special Publication 800-53, Revision 1: Recommended