DNSSEC
Why?

Presented by

Olaf Kolkman (NLnet Labs)

and

Alain Aina(TRS)

Kuala Lumpur, 28-30 August 2007

The Material

- Based on material developed while I was with the RIPE NCC.
- I also borrowed heavily from other sources
  - Organizations and individuals
- They are acknowledged for allowing me to re-use this material

Introducing DNSSEC

Why DNSSEC

- Good security is multi-layered
  - Multiple defense rings in physical secured systems

Bourtange, source Wikipedia

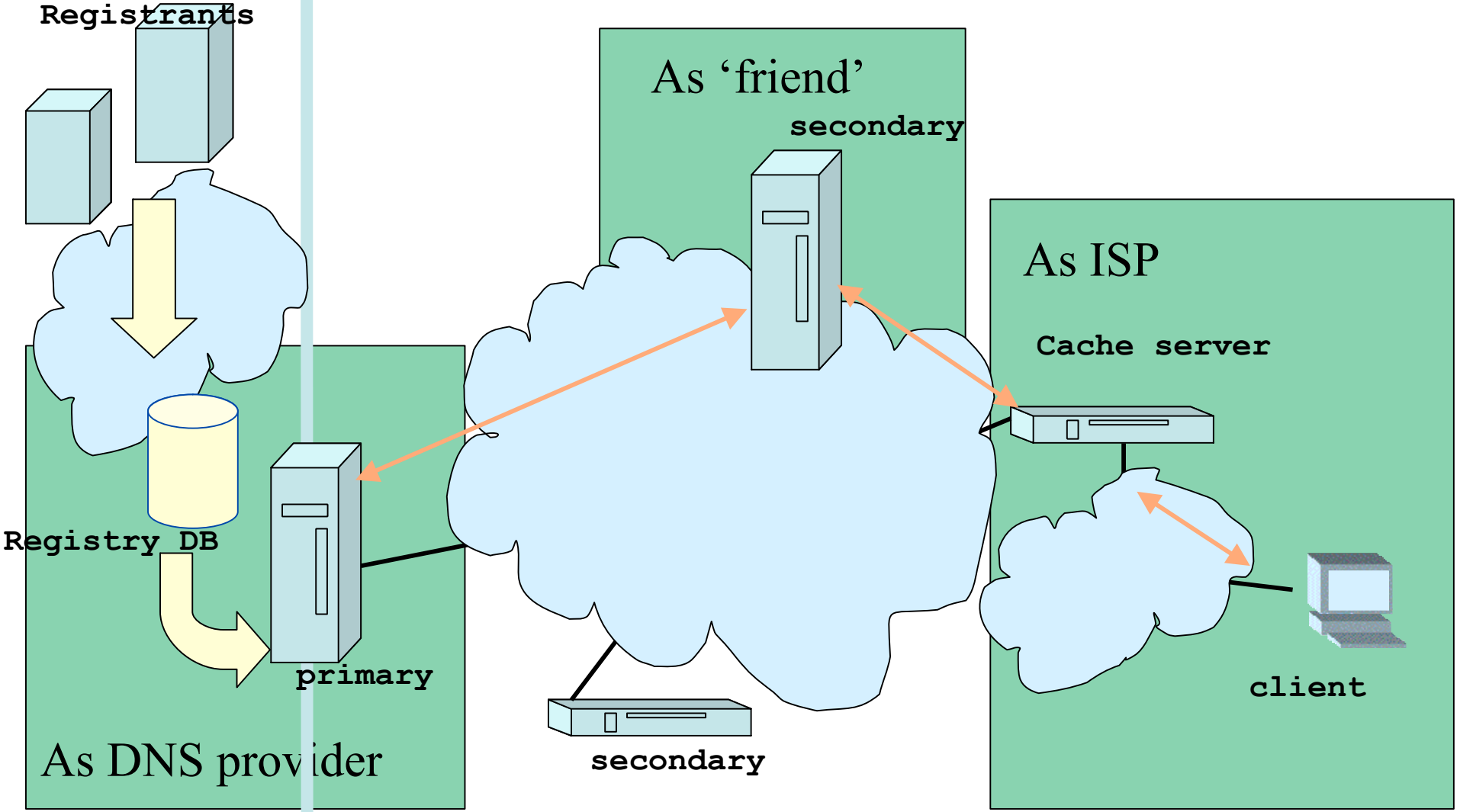
Why DNSSEC

- 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

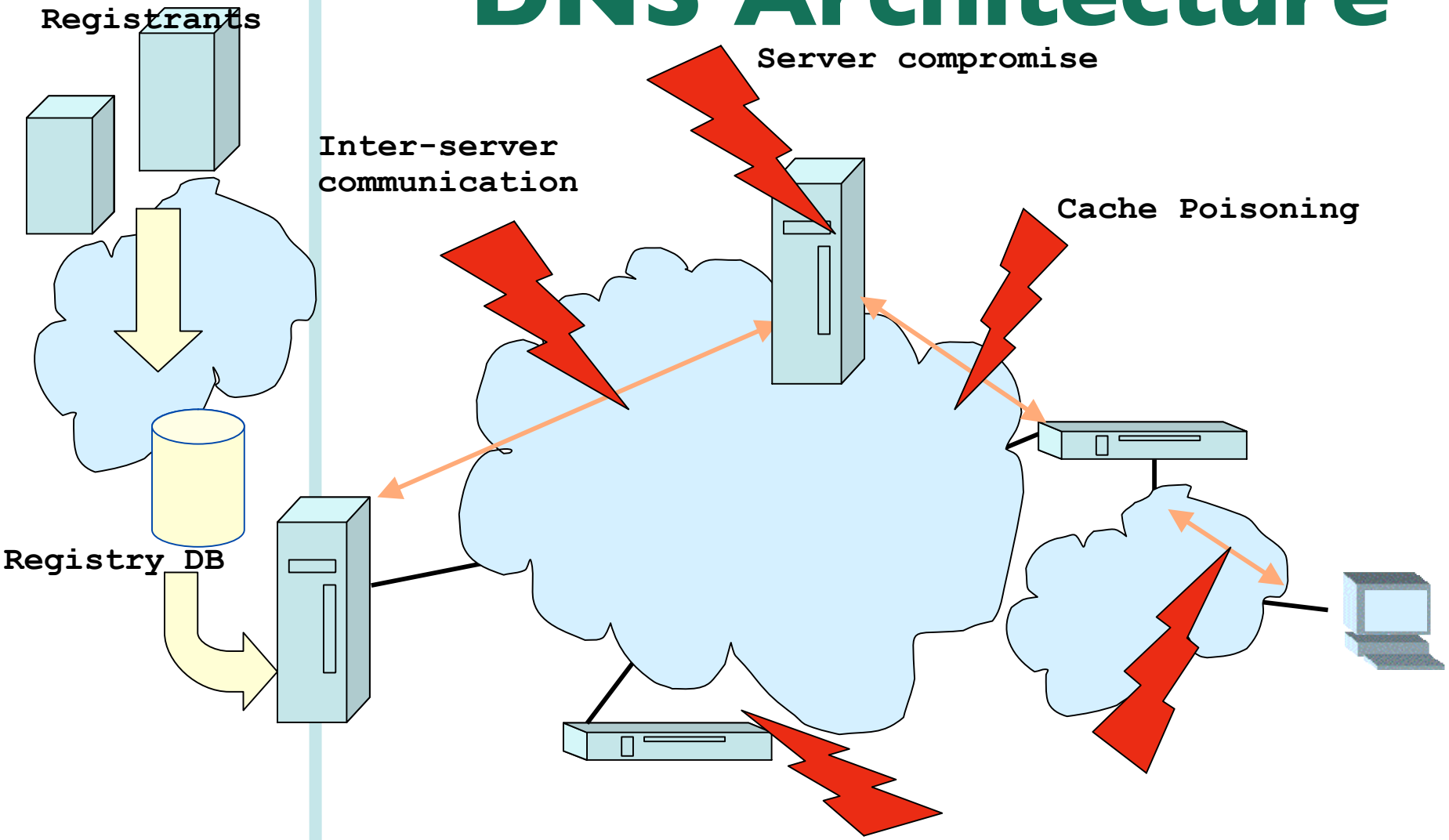
The Problem

- 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
  - 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

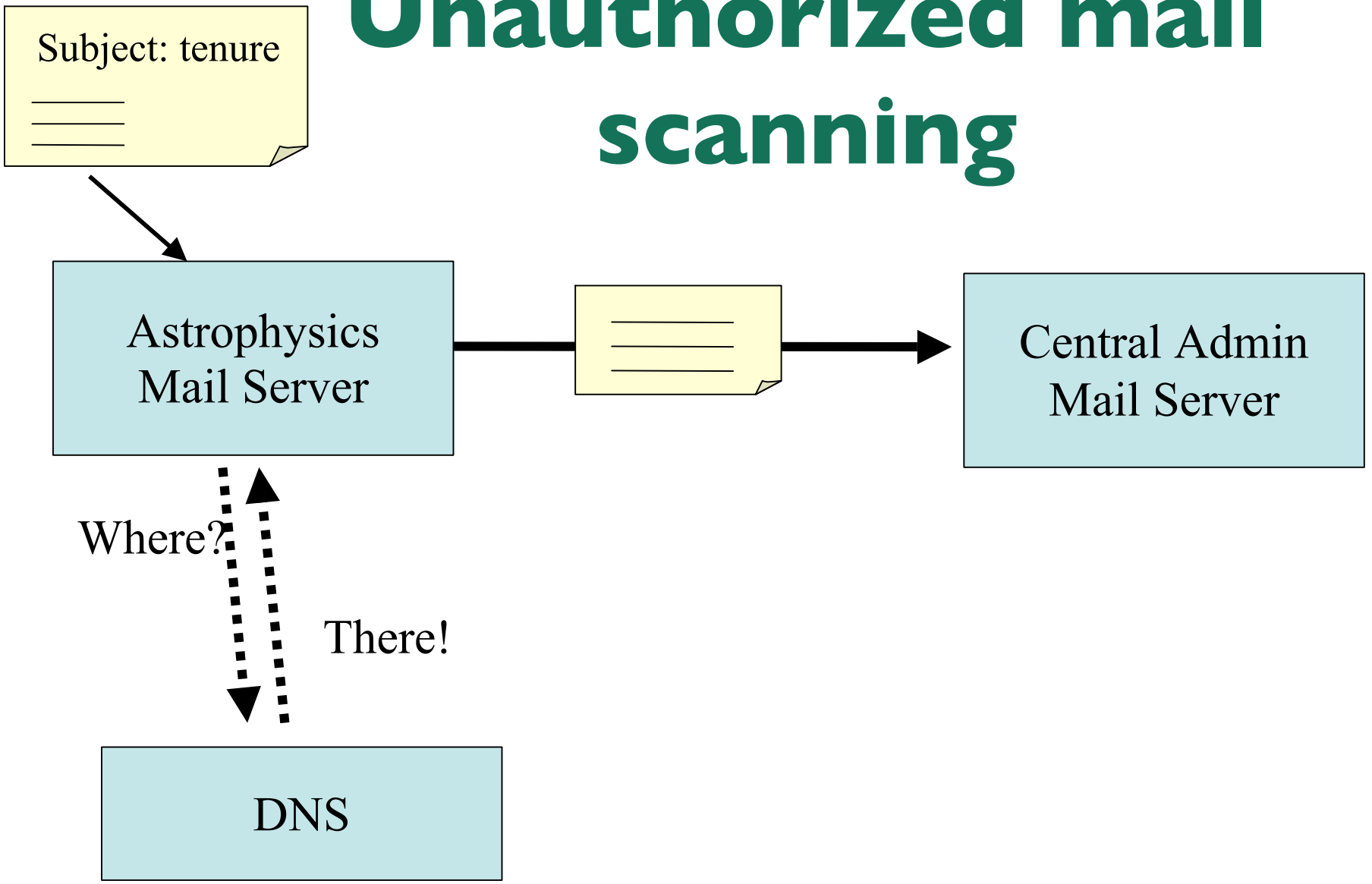


DNS Architecture

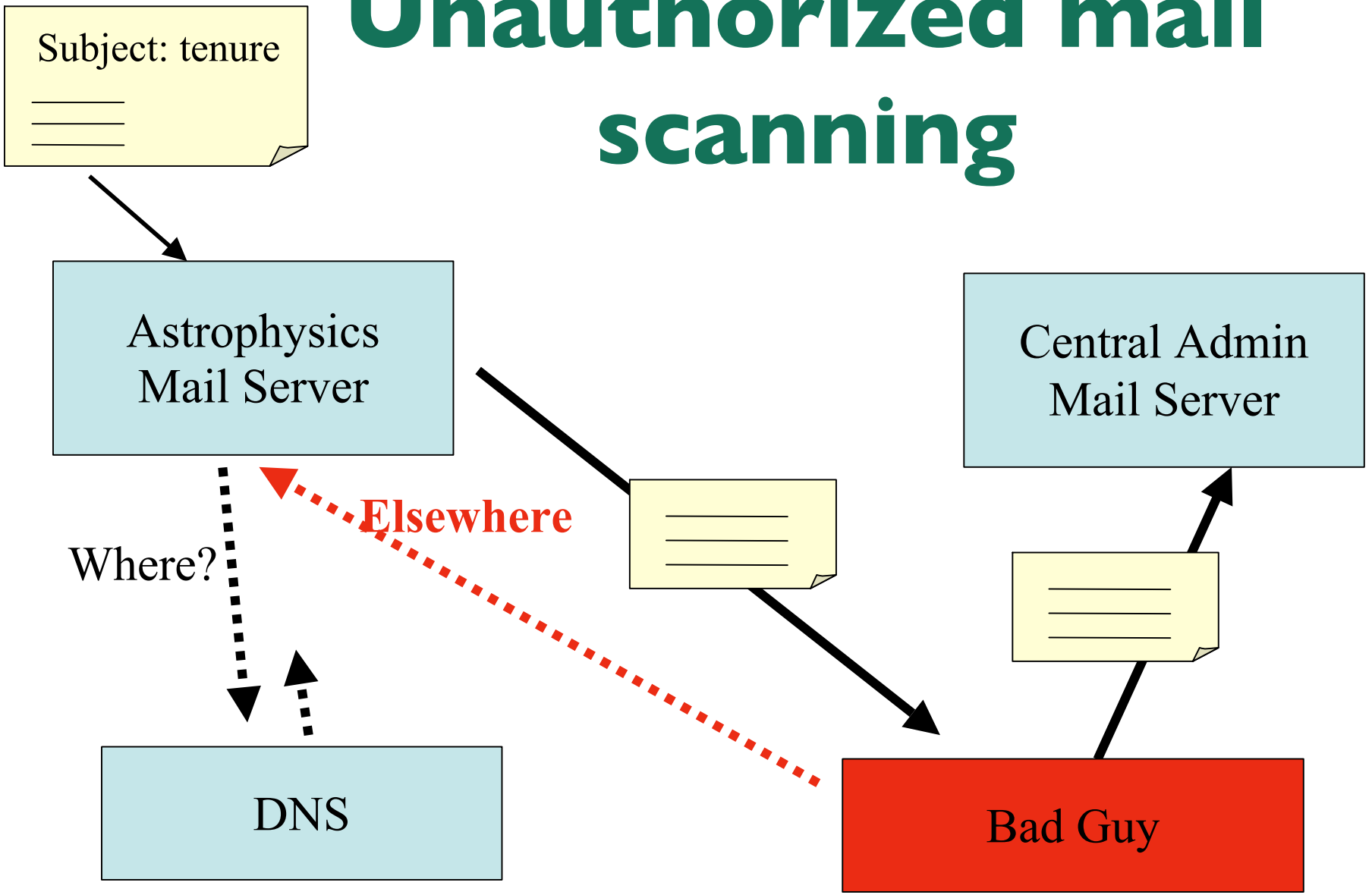


Provisioning DNS Protocol

Example: Unauthorized mail scanning



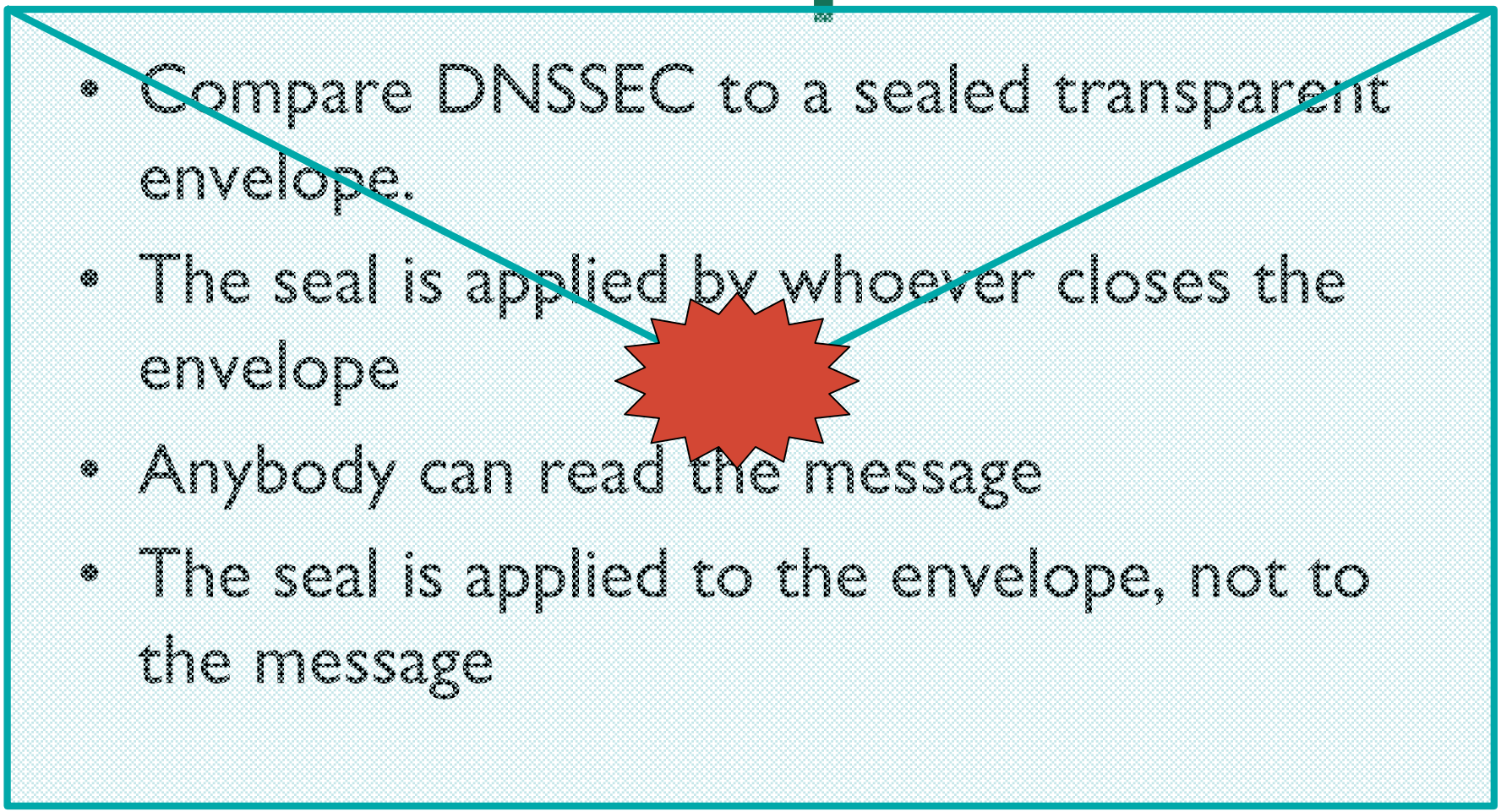
Example: Unauthorized mail scanning



Where Does DNSSEC Come In?

- DNSSEC secures the name to address mapping
  - Tranport 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 secondary benefits

- 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
  - See 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"

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

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

Methods to prevent Cache Poisoning

<Qname, Qclass, Qtype, IP-quad, query-ID>

- Careful matching against all of the above
  - Utilize the maximum amount of variation possible
  - Not predictable
- Qname: 0x20 proposal
  - Qname: Www.ExaMpLE.coM.

Wait-a-minute

- Is DNSSEC still needed?
  - Aren't the methods to prevent cache poisoning sufficient?
    - Yes, prudently written software makes the possibility to poison caches less likely
  - Recognize an arms-race?
    - Only untill the next clever trick is announced.
    - DNS is inherently insecure
- The other attack vectors still exist
  - Access to the wire e.g. hijack of DNS server addresses
  - Secondary server access

Summary

DNSSEC is essential for good layered security
DNS protocol intrinsically easy to attack
DNSSEC and Transport security

Questions?