

100010010100101010000010110001000001111100101
1101011001010110110010110011001011101100000
1001101011111110001111011010001111110101
11111010100001111010100100100111110101
10010100101110000011101000010000010000000
1000011101101001110100101101100001001
01000101101100101101000010001001000000
0000111010011011011000111111010101
0001010111010001100111000111100101
001011100100100110001011011001001
0100101001100001110000010011001
100100101000111110010101001001
0111000101110011101001001001
1101101011101111011001001
100010110010100101001001001
0100011001001001001001001001
011101101110011001100110011001
110011000001100000110000011000001
0101111000001100000110000011000001
0011010101010101010101010101010101010101
0010100000000000000000000000000000000000
1111000000000000000000000000000000000000
1011000000000000000000000000000000000000

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

100010010100101010000010110001000001111100101
11010110010101101100101100110010111011100101
1001101011111110001111011010001111110101
11111010100001111010100100100111110101
1001010010111000001110100001000001000001
1000011110110100111010010110110000101
0100010110110010110100001000100100001
0000111010011011011100011111101101
0001010110100011001110001111100101
00101110010010011000101101100101
010010100110000111000010011001
100100101000111110010101
01100010111001110100101
110110101110111101101
100010110010100101001
010001100100100101
0111011011100101
110011000001100001
010111100001100001
0011010101
00101000001

Introducing DNSSEC

Why DNSSEC

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



Bourlange, source wikipedia

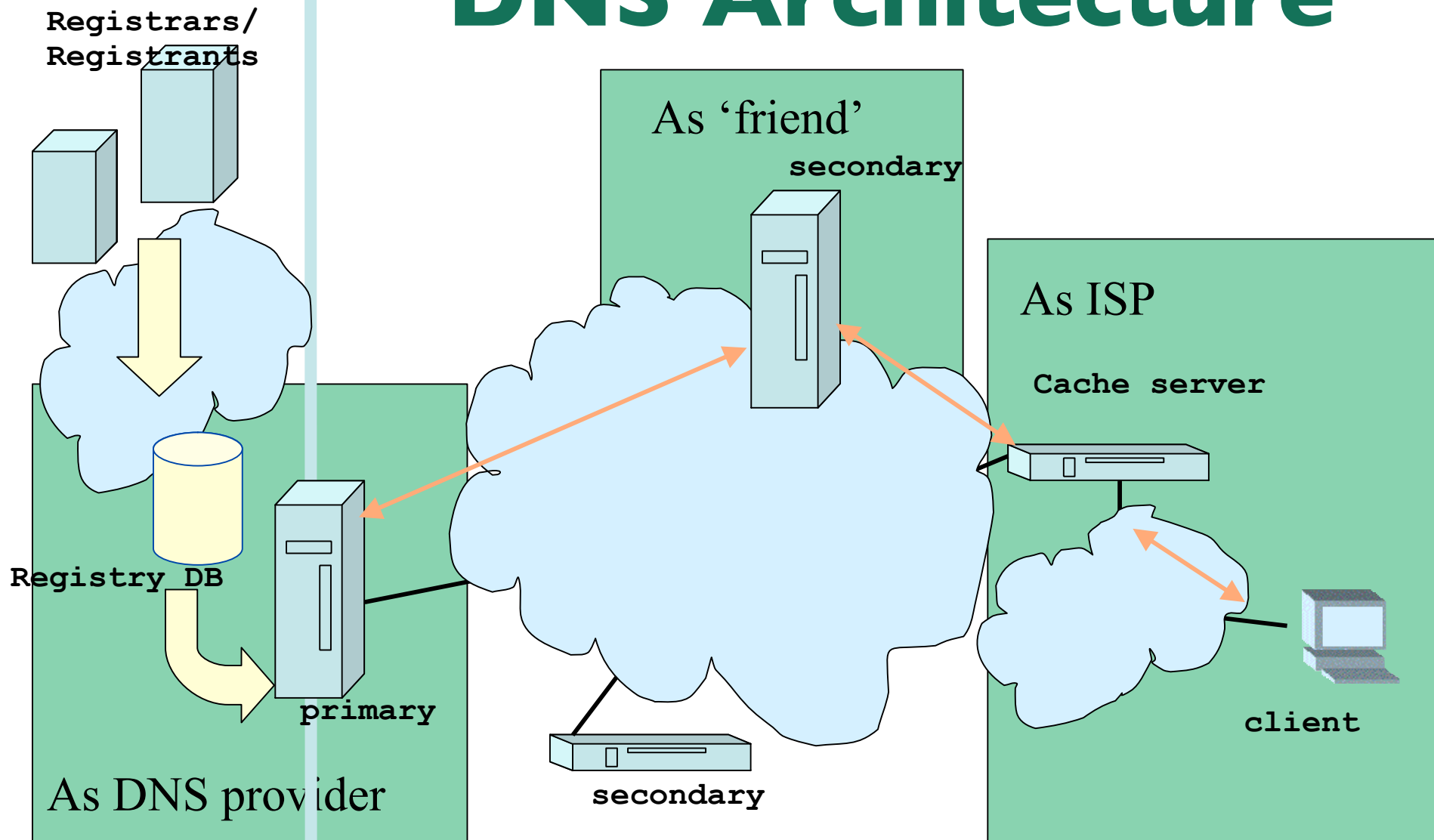
Why DNSSEC

- 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 than others
 - Vulnerabilities in DNS software make attacks easier (and there will always be software vulnerabilities)

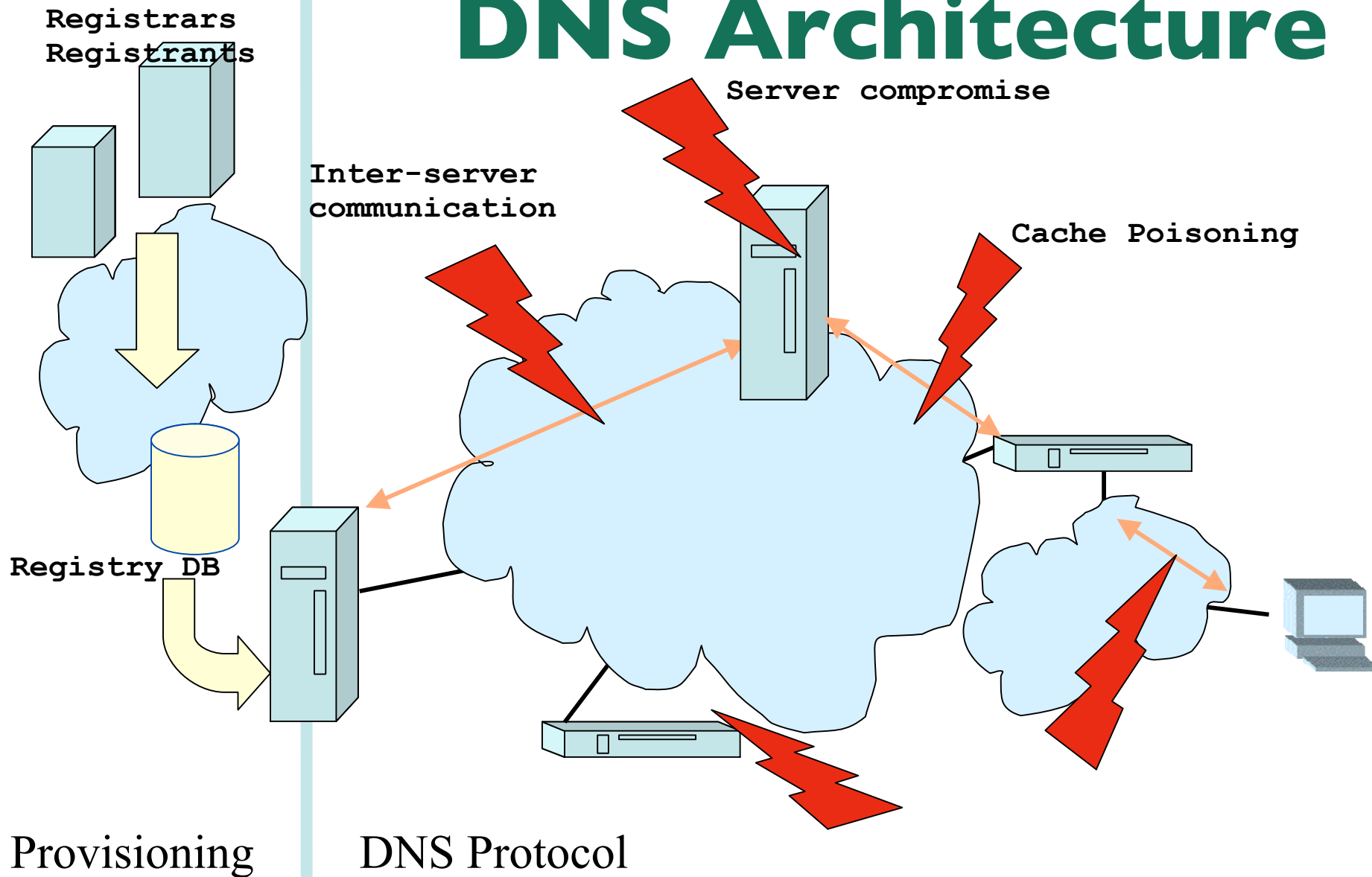
DNS Architecture



Provisioning

DNS Protocol

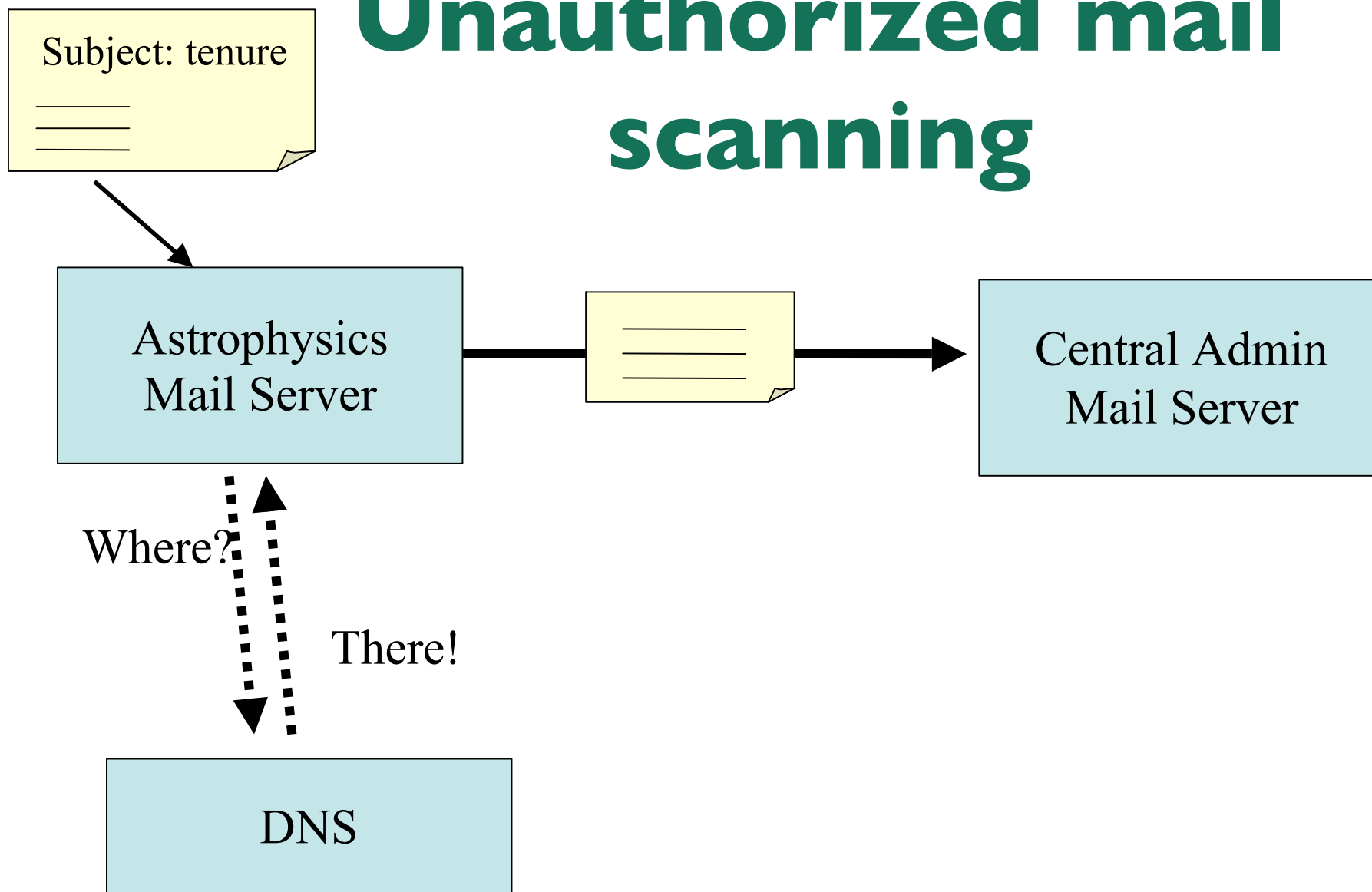
DNS Architecture



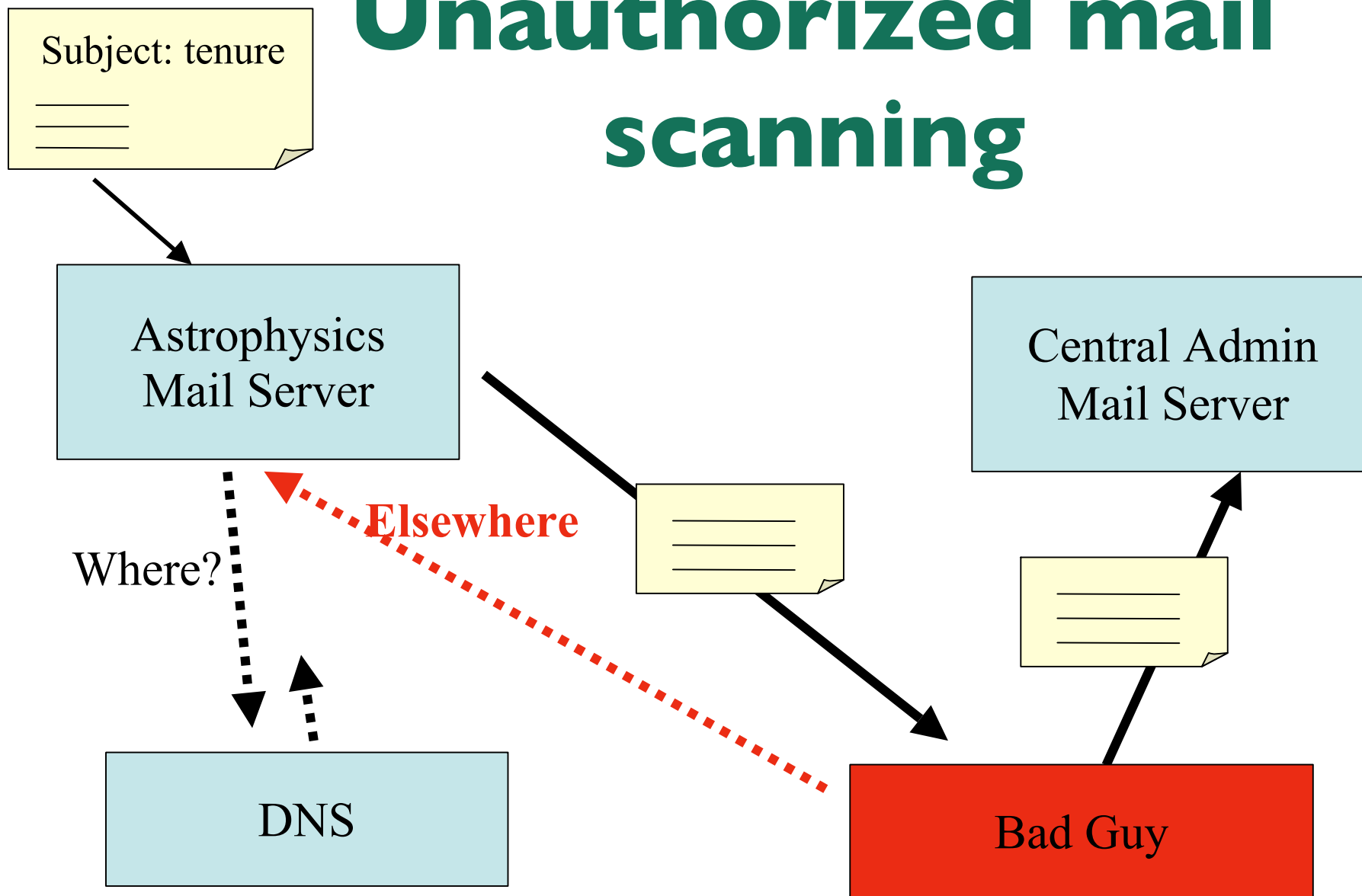
Provisioning

DNS Protocol

Example: Unauthorized mail scanning



Example: Unauthorized mail scanning

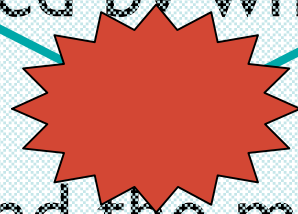


Where Does DNSSEC Come In?

- DNSSEC secures the name to address mapping
 - 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 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 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 until 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?