DNSSEC Deployment:

Where Is It &
What Are the Issues

Russ Mundy

Principal Networking Scientist

mundy@sparta.com

mundy@tislabs.com

410-430-8063

DNSSEC Deployment

- Extremely High-level DNSSEC Overview
  - Provides DNS users with the capability to cryptographically verify answers to DNS queries
    - Integrity of information received
    - Source authenticity of the information
  - Provides a ‘real basis’ for users to use DNS like they do today!
    - Most users just accept and use DNS information without any concern about whether or not it’s correct

Do the Problems Still Exist?

- Anti-Spam and anti-phishing technologies
  - Technologies that use the DNS to mitigate spam and phishing: $$$ value for the ‘Bad Guys’
- StockTickers, RSS feeds
  - Usually no source authentication but supplying false stock information via a stockticker or via a news feed can have $$$ benefit for attacker
- ENUM
  - Mapping telephone numbers to services in the DNS
    - As soon as there is some incentive

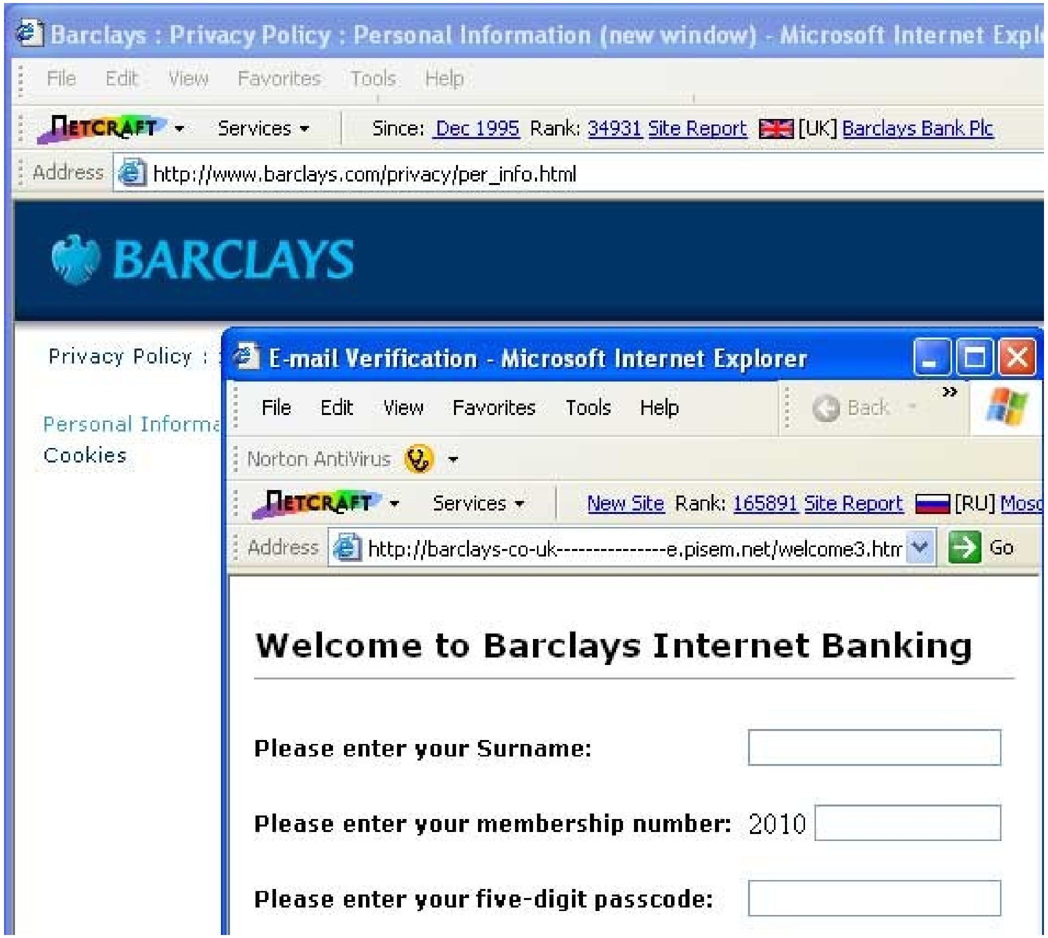
Recent Attacks: Barclays Wildcard

- In this attack, a version of pharming, a user is presented with an encoded URL for a destination, which looks correct on common browsers
  - Is that a bug or a feature?
- Even if users become weaned from reacting to pharming email, this URL might show correctly in dynamic click-ads
- URL resolves to a redirector site in Russia

URL with Encoded Redirector

- http://barclays.co.uk|snc9d8ynusktl2wpqxzn1a
- Possible solutions:
  - “Fix” all browsers and people against these attacks (and each new one that gets invented)
  - Make the infrastructure generally robust against all redirection attacks
- The second option is best

Barclays Wildcard


Barclays : Privacy Policy : Personal Information (new window) - Microsoft Internet Expl
File Edit View Favorites Tools Help
NETCRAFT Services
Since: Dec 1995 Rank: 34931 Site Report [UK] Barclays Bank Plc
Address http://www.barclays.com/privacy/per_info.html
BARCLAYS
Privacy Policy :
Personal Informa
Cookies
E-mail Verification - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Norton AntiVirus
NETCRAFT Services
New Site Rank: 165891 Site Report [RU] Mosc
Address http://barclays-co-uk--------------e.pisem.net/welcome3.htm
Go

Welcome to Barclays Internet Banking

Please enter your Surname:

Please enter your membership number: 2010

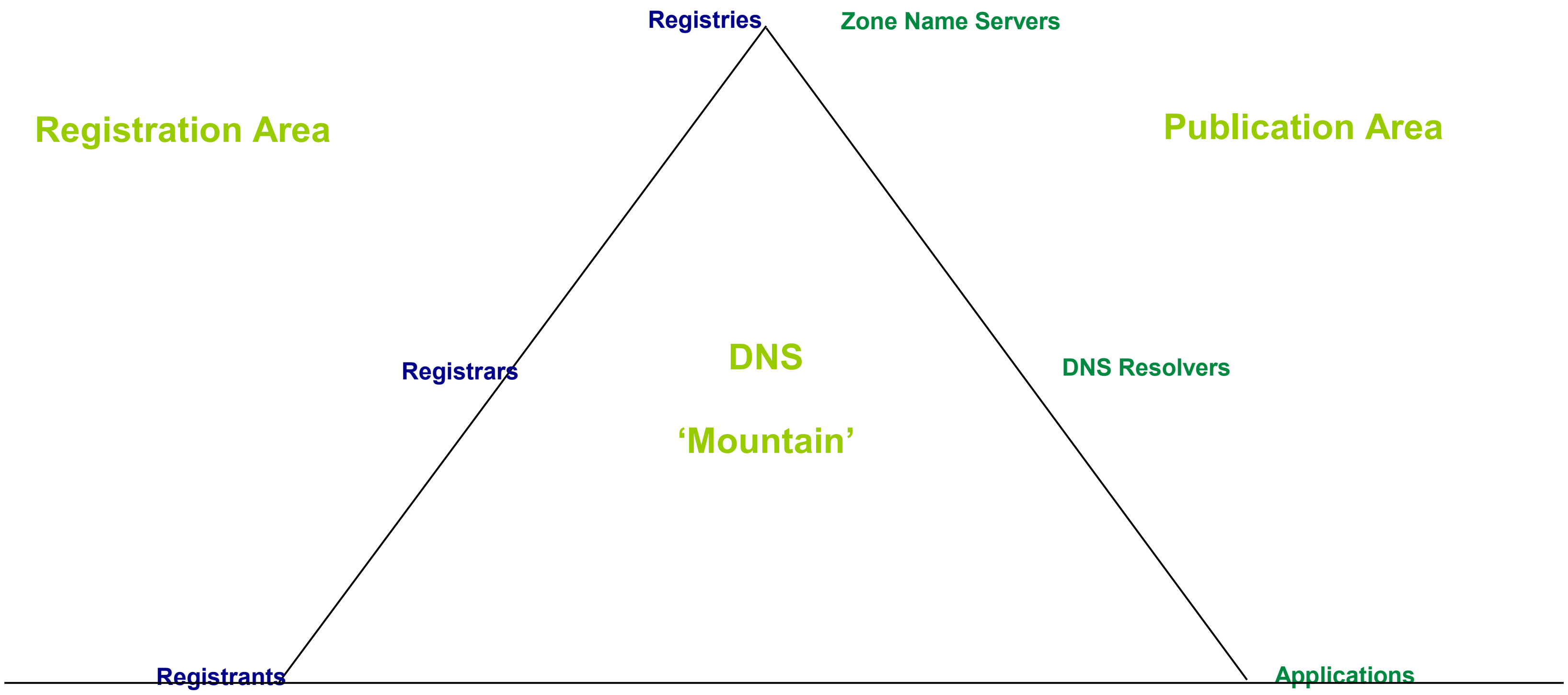
Please enter your five-digit passcode:

http://news.netcraft.com/archives/2005/03/07/phishers_use_wildcard_dns_to_build_convincing_bait_urls.html

Do the Problems Still Exist?

- DNS cache poisoning attacks are an old problem but seem to continue unabated
  - Symantec products found to be vulnerable in March 2005
  - Microsoft and BIND cache poisoning attacks in April 2005
  - DNS bots in May 2005
  - Multiple targeted attacks in early 2006
- Details on a recent large DNS cache poisoning attack at http://isc.sans.org/presentations/dnspoisoning.php

Where Does DNSSEC Fit?



Registries

Zone Name Servers

Registration Area

Publication Area

Registrars

DNS

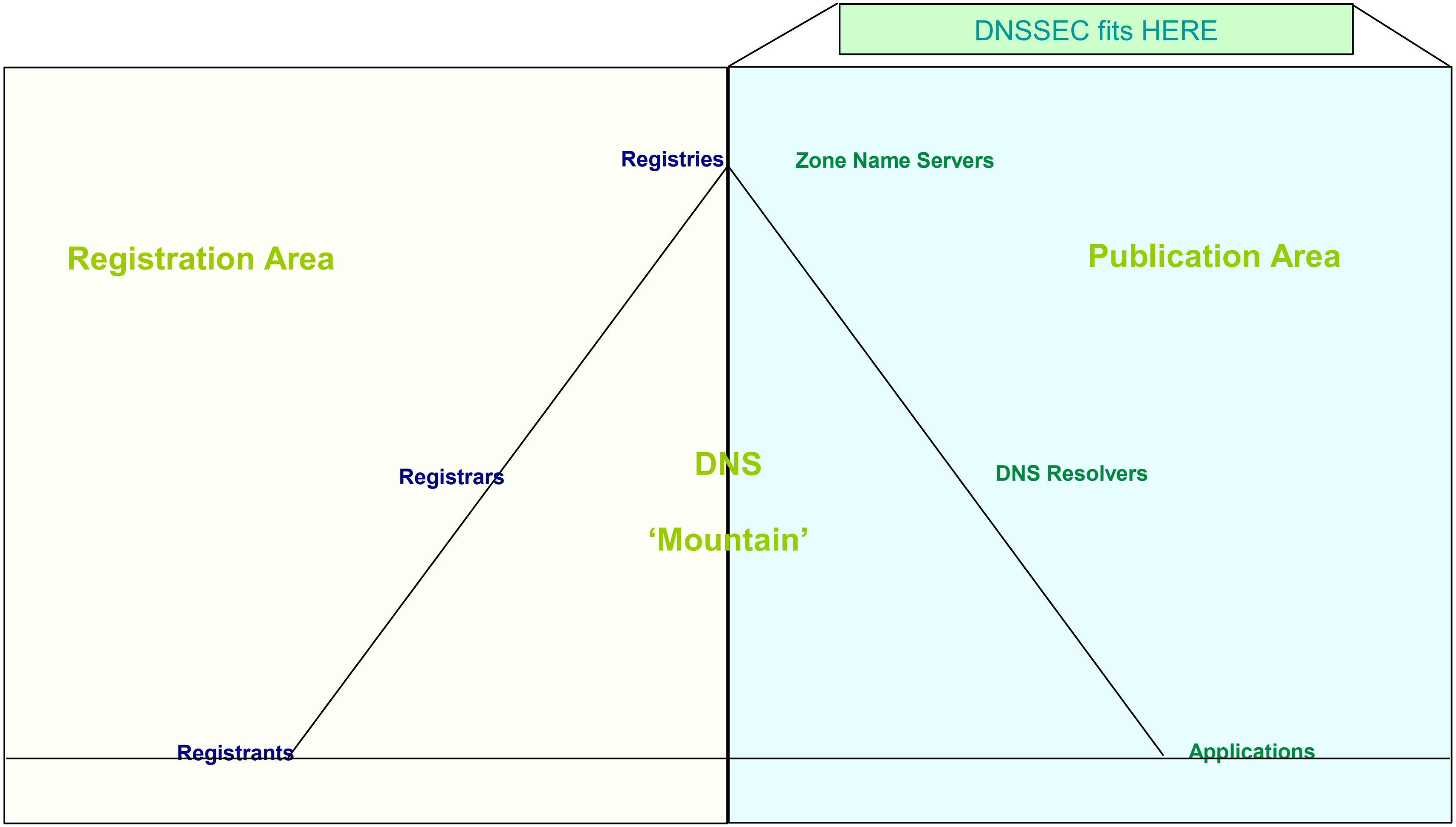
'Mountain'

DNS Resolvers

Registrants

Applications

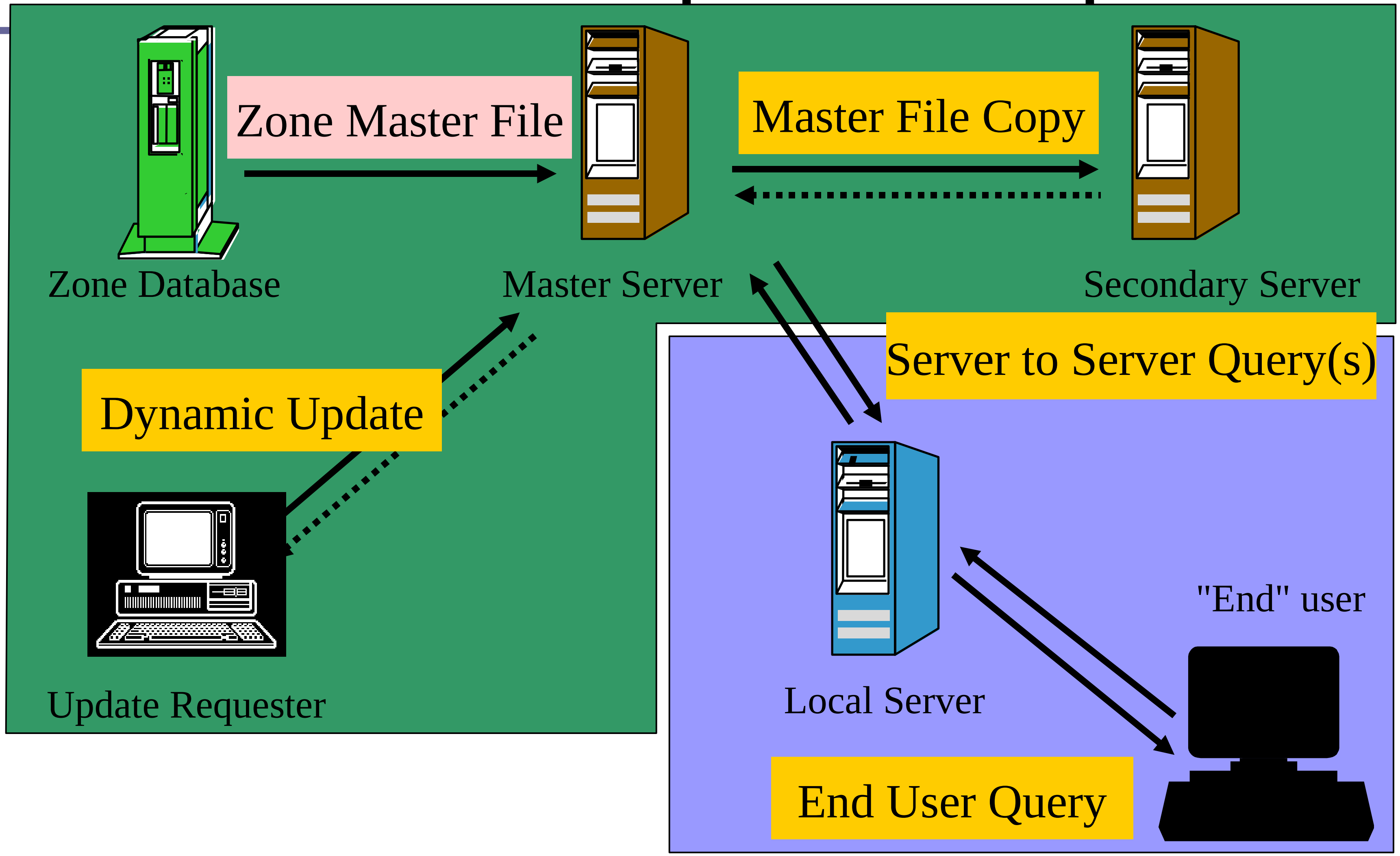
Where Does DNSSEC Fit? (cont.)



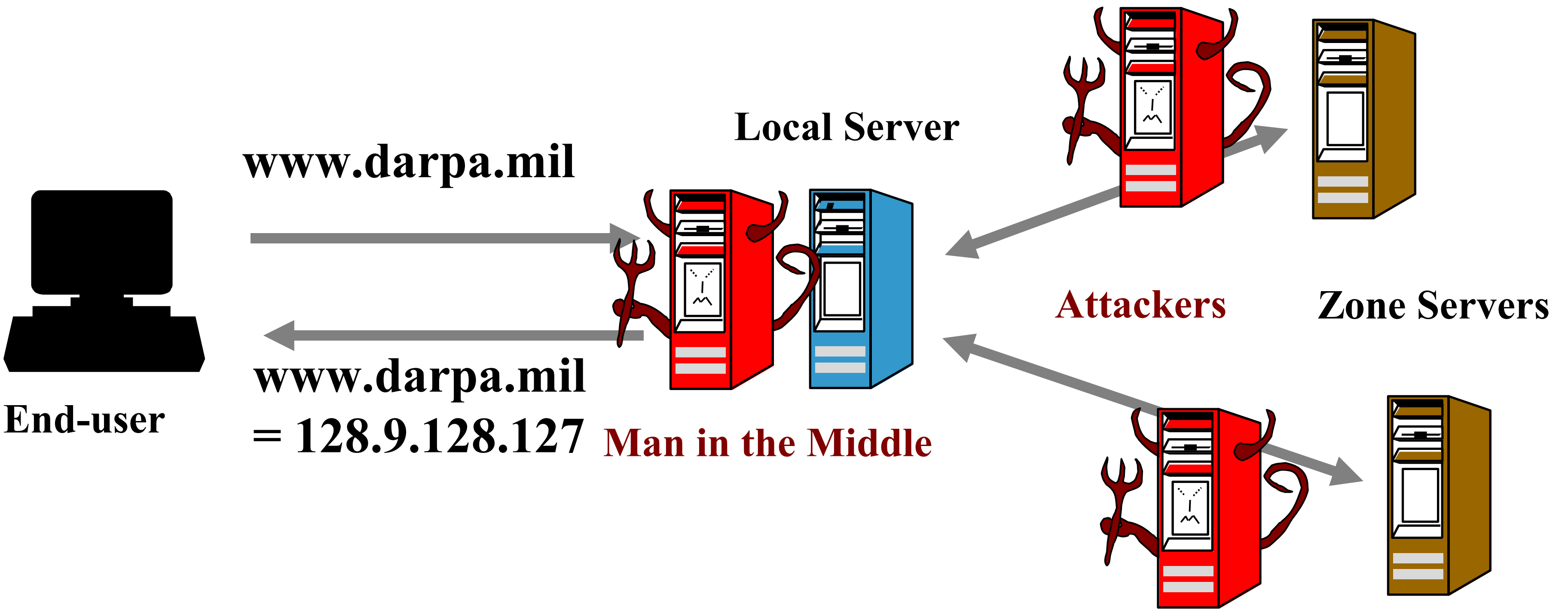
DNSSEC Myth Buster Slide

- DNS authoritative-only name servers are NOT required to perform any cryptographic functions
  - DNSSEC records should normally be created with same process/machinery as master file.
- In some environments (e.g., signed dynamic dns zone), operator may choose to do crypto functions on authoritative server.

Zone Data - Input & Output



Some DNS Vulnerabilities



Forged/compromised data

Local Server

www.darpa.mil

Attackers

Zone Servers

End-user

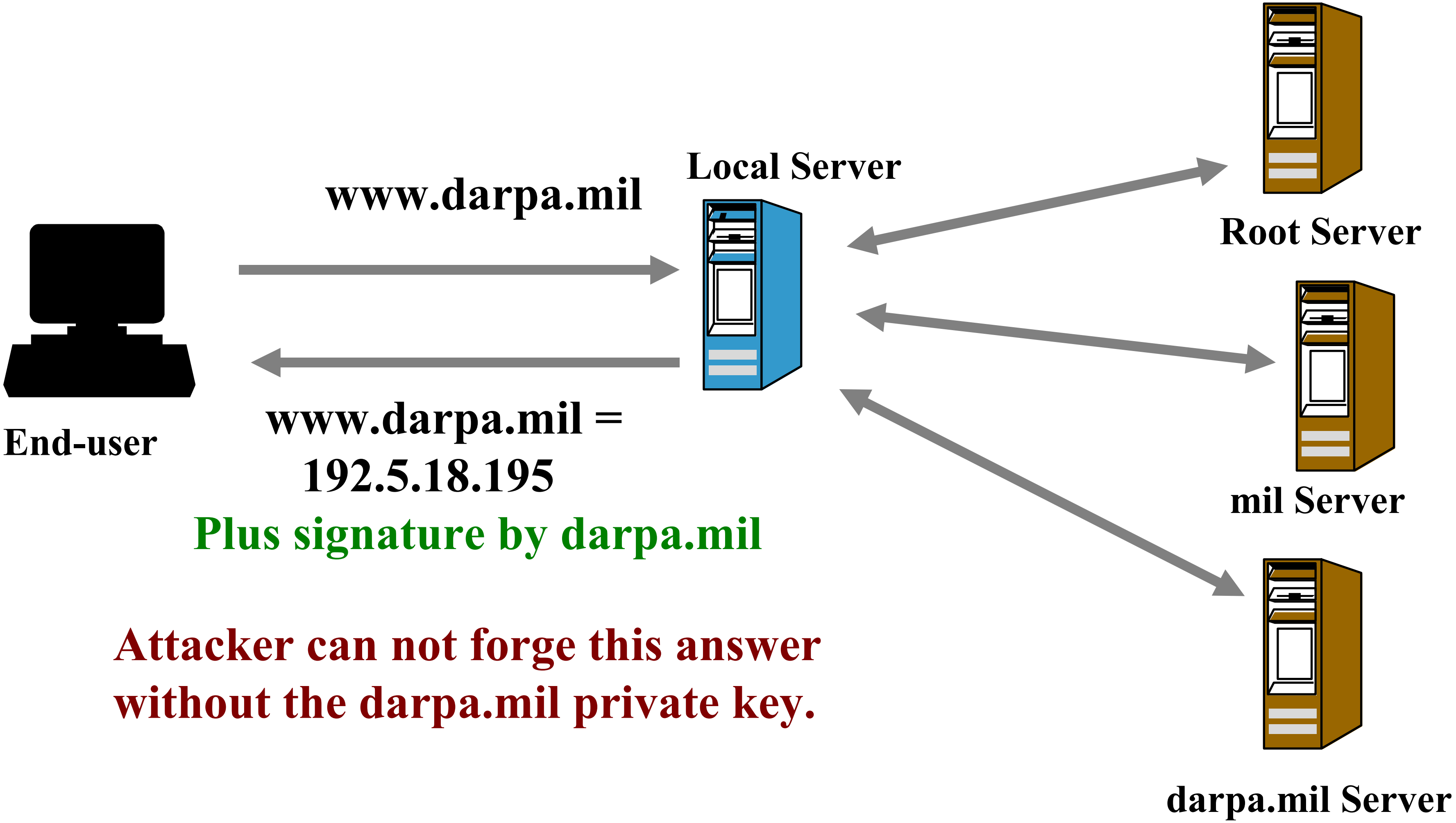
www.darpa.mil
= 128.9.128.127

Man in the Middle

Cache poisoning

Actually www.darpa.mil = 192.5.18.195.
But how do you determine this?

Secure DNS Query and Response



www.darpa.mil = 192.5.18.195

Plus signature by darpa.mil

Attacker can not forge this answer without the darpa.mil private key.

DNSSEC Hypersummary

- Each DNS zone signs their data with their private key.
  - Signing should be done with zone data preparation
- User queries are answered with:
  - the requested information;
  - plus DNSSEC data for the requested information.
- Users authenticate responses with trusted key(s)
  - At least one trusted public key is pre-configured
  - Validation done with pre-configured key or keys learned via a sequence of queries to the DNS hierarchy.
- Enables and supports other security technologies

DNSSEC Deployment

So What Has Been Happening
with
DNSSEC Deployment?

DNSSEC in Europe: RIPE

- The European infrastructure services provider, RIPE NCC, based in the Netherlands, has a major initiative in place to deploy DNSSEC in zones it manages
- Details are at https://www.ripe.net/rs/reverse/dnssec/
- How-to guide at https://www.ripe.net/projects/disi/dnssec_howto/

DNSSEC in Europe: Sweden

- In November 2005 the Swedish national registry (.se) was the first ccTLD – country code top level domain – to provide DNSSEC-capable service
- Details: http://dnssec.nic.se/
- Questions may be addressed to dnssec-info@nic.se

DNSSEC in Europe: Russia

- R01 (http://www.r01.ru/), a Russian registrar, has a signed copy of the .ru zone available on their name server
  - ns.dnssec.ru (195.24.65.7)
- Registrants with a .ru domain using R01 as a registrar can sign their own zones
  - R01 will provide secure delegation in the signed copy of the .ru zone
- Additional information on the signed zone and how it can be used can be found at http://www.dnssec.ru

DNSSEC in Asia

- DNSSEC summit and workshop during APRICOT 2005, Kyoto
  - http://www.apricot.net/apricot2005/worksho
  - http://www.psg.com/~mankin/DNSSEC-Kyo

US DHS DNSSEC Deployment Initiative

- DHS Science and Technology (S&T) Directorate sponsors several Internet security initiatives including
  - DNS Security Extensions
  - Secure Protocols for the Routing Infrastructure
  - Protected Repository for the Defense of Infrastructure against Cyber Threats
- DHS cannot secure the Internet by itself
  - But is taking a leadership role in facilitating public-private partnerships that will result in a more secure Internet
  - Also leading an effort to sign the .gov zone

DNSSEC Initiative Activities

- Roadmap published in February 2005
  - http://www.dnssec-deployment.org/roadmap.php
- Multiple workshops held world-wide
- Monthly newsletter
  - http://www.dnssec-deployment.org/news/dnssecthismonth/
- DNSSEC tools available at
  - http://www.dnssec-tools.org/
- DNSSEC testing tools developed by NIST
  - http://www-x.antd.nist.gov/dnssec/

DNSSEC in the United States

- Formal publicity and awareness plan under development by DHS/S&T CSRDC
- US civilian government (.gov) developing policy and technical guidance for secure DNS operations and beginning deployment activities at all levels.
- The ".us" and ".mil" zones are also on track for DNSSEC compliance
- New DNSSEC guidance was proposed for inclusion in FISMA, NIST 800-53r1
  - http://www.csrc.nist.gov/publications/nistpubs/

Some DNSSEC Next Steps

- Work with folks interested in deploying DNSSEC to facilitate that deployment
  - Focus on high-benefit deployers as much as possible
  - Improve dnssec-deployment web site be more useable by various types of deployment groups, e.g., DNS service providers, ISPs, user enterprizes
  - Provide tools needed to facilitate deployment
  - Continure work open DNSSEC issues
    - Performance, root related actions, key rollover, zone walking, algorithm & code rollover, application issues, zone operator resources, business & usage cases

Background Information and Contributors

- For lots of detailed information:
  - www.dnssec-deployment.org
  - www.dnssec-tools.org
  - www.dnssec.net
- Authors of materials in this presentation (all from dnssec-deployment working group)
  - Amy Friedlander (Shinkuro)
  - Olaf Kolkman (Netlabs.nl)
  - Ed Lewis (Neustar)
  - Allison Mankin
  - Russ Mundy (Sparta)
  - Marcus Sachs (SRI)

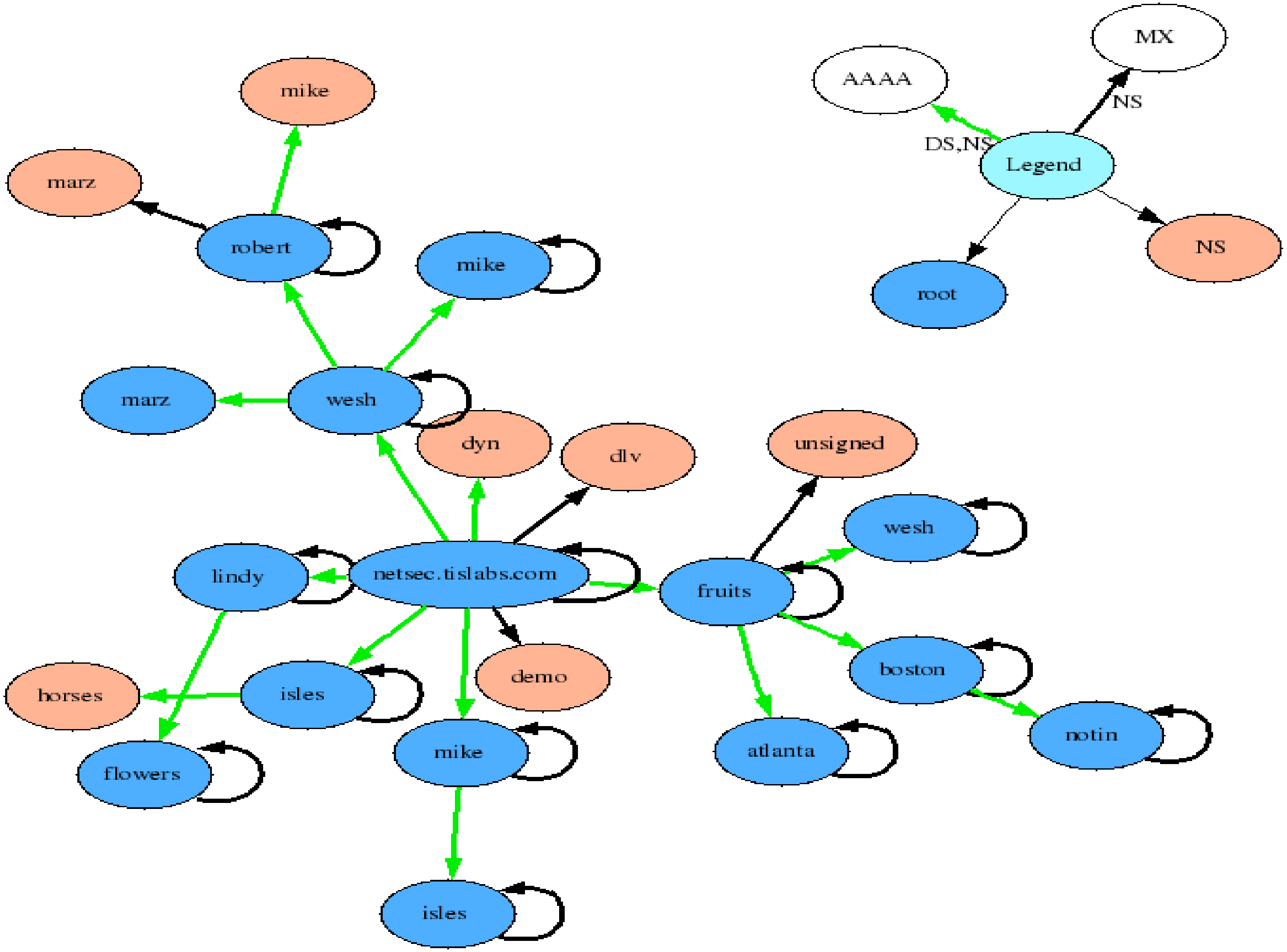
Questions/Comments....

Backup Slides
for
Tools & Applications

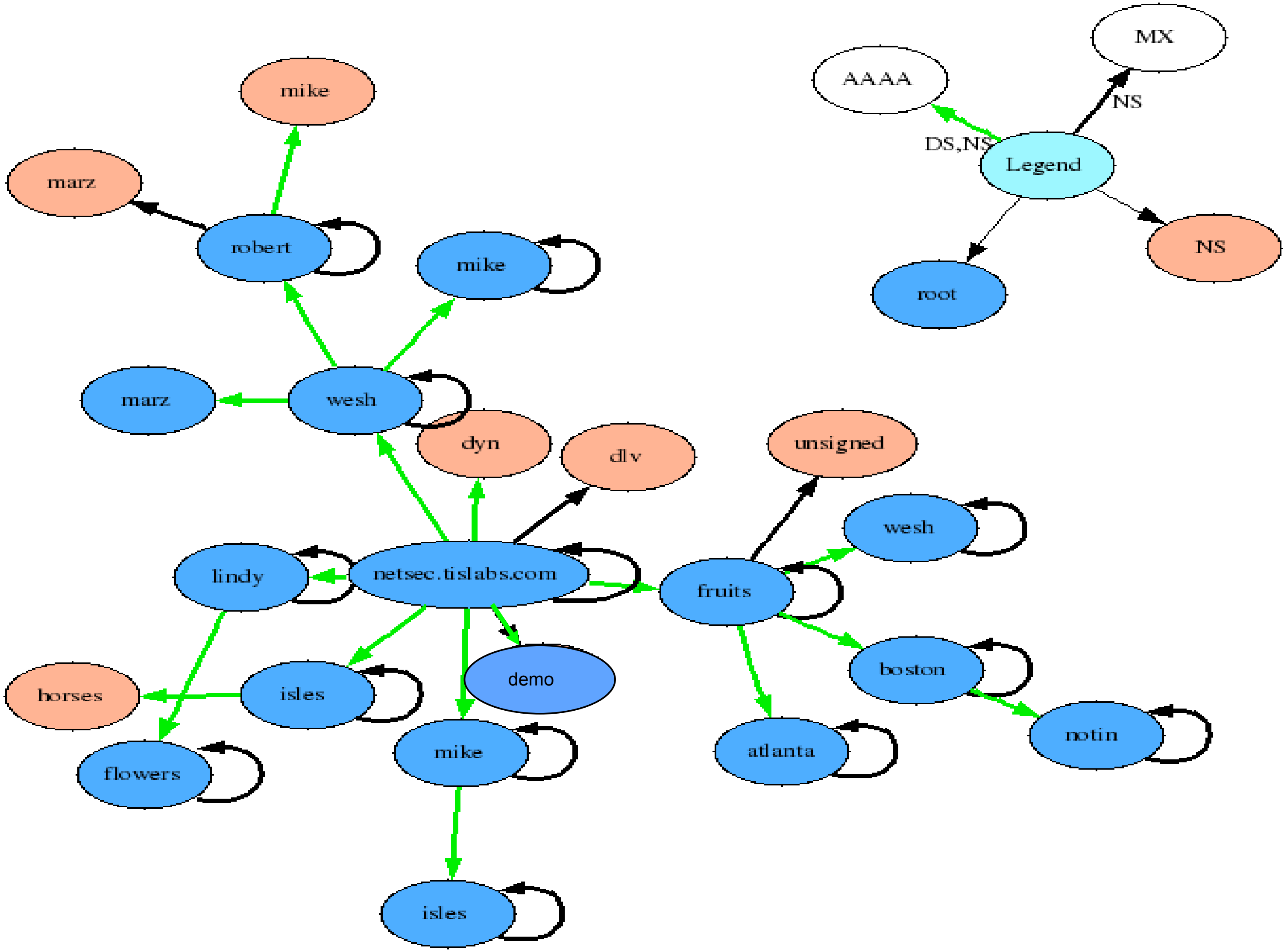
Zonesigner makes life simpler

- One step process
- Default setting does the “right thing” most of the time
- Details of signing operations and keys used are hidden, so zone signing (and re-signing) operations are less error prone
- Easy installation - has only a few dependencies.

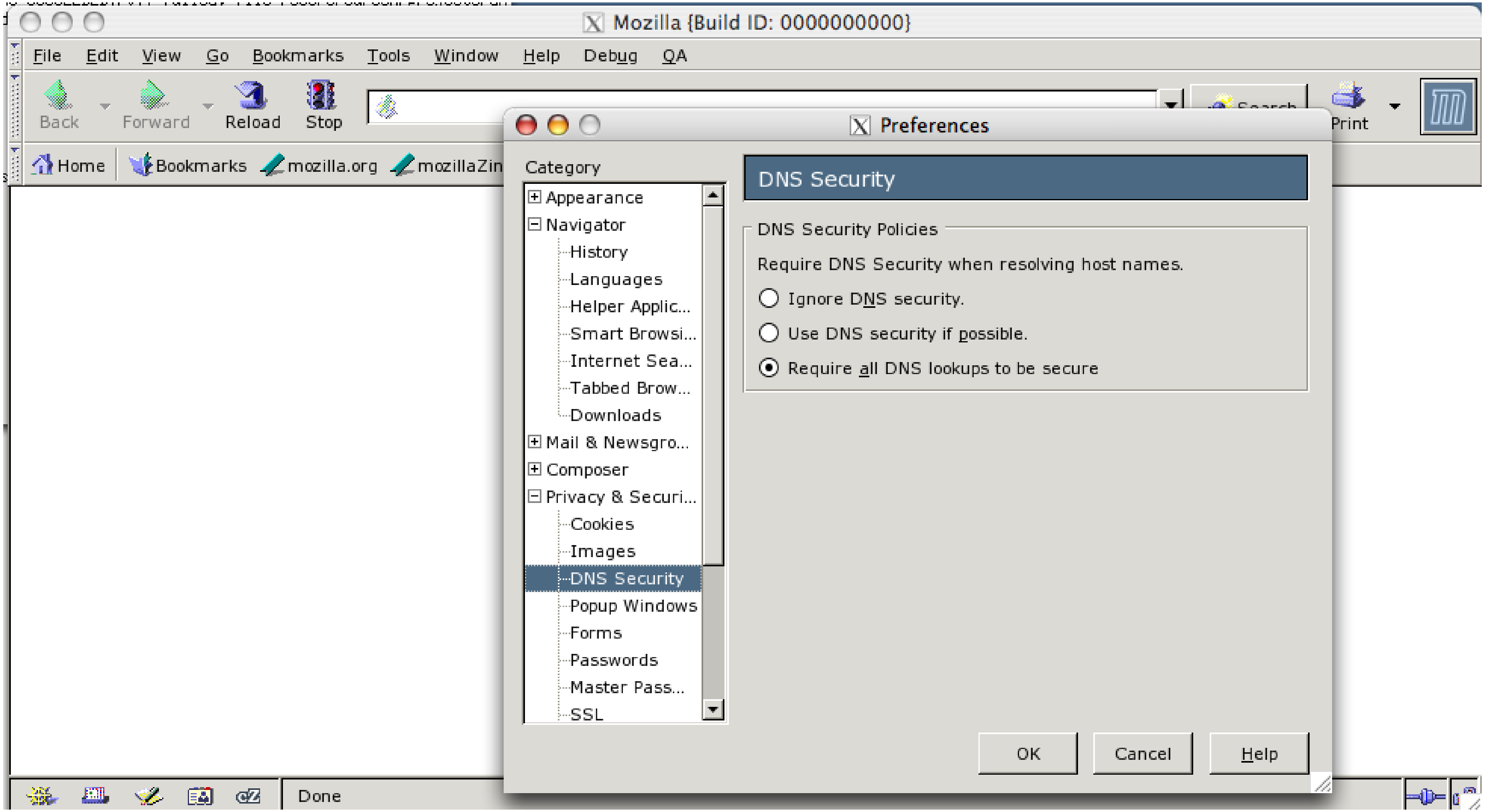
Use Mapper to view zone status (before)



Use Mapper to view zone status (after)



Enable DNSSEC in mozilla



DNS Security

DNS Security Policies

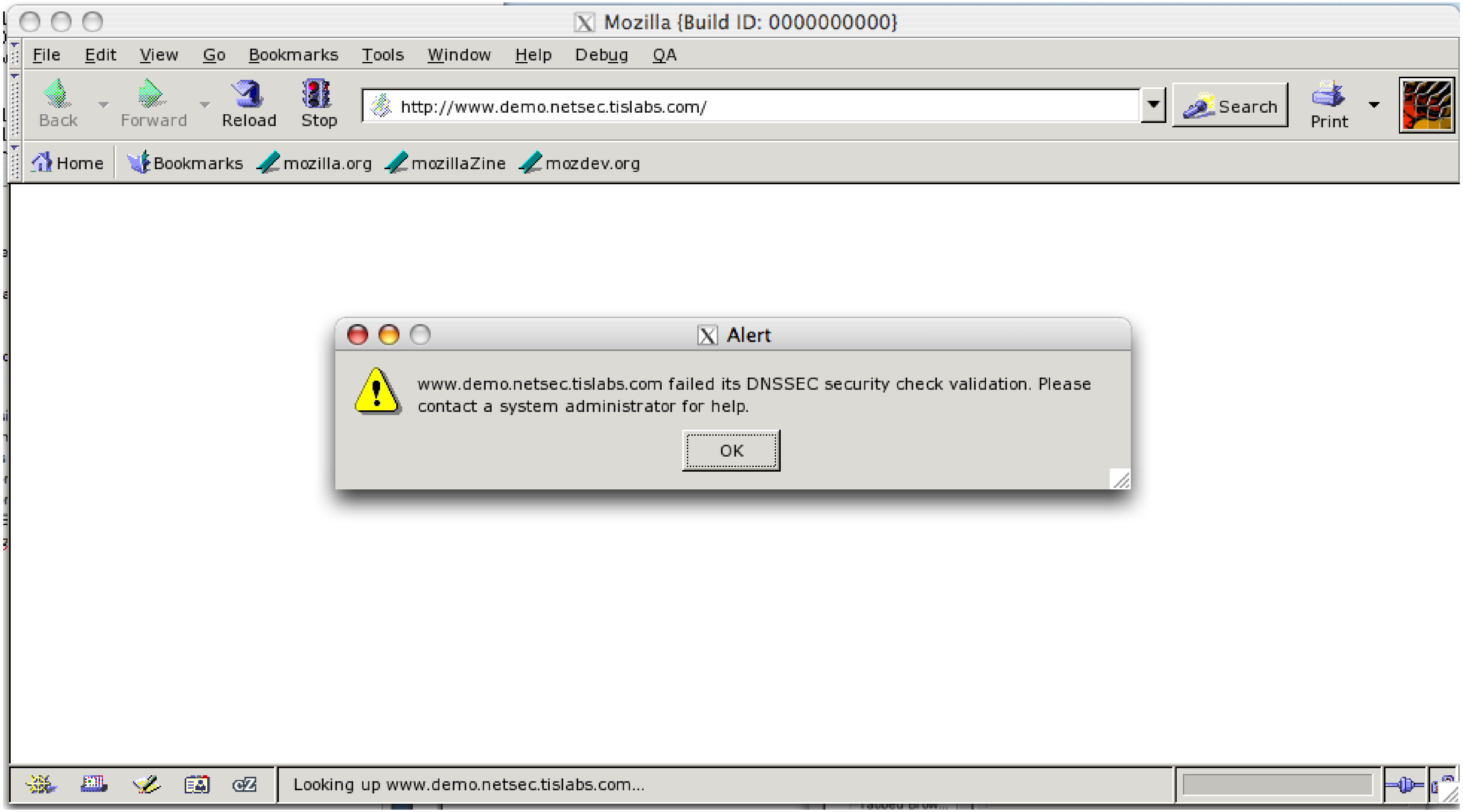
Require DNS Security when resolving host names.

○ Ignore DNS security.

○ Use DNS security if possible.

● Require all DNS lookups to be secure

Mozilla detects validation failures

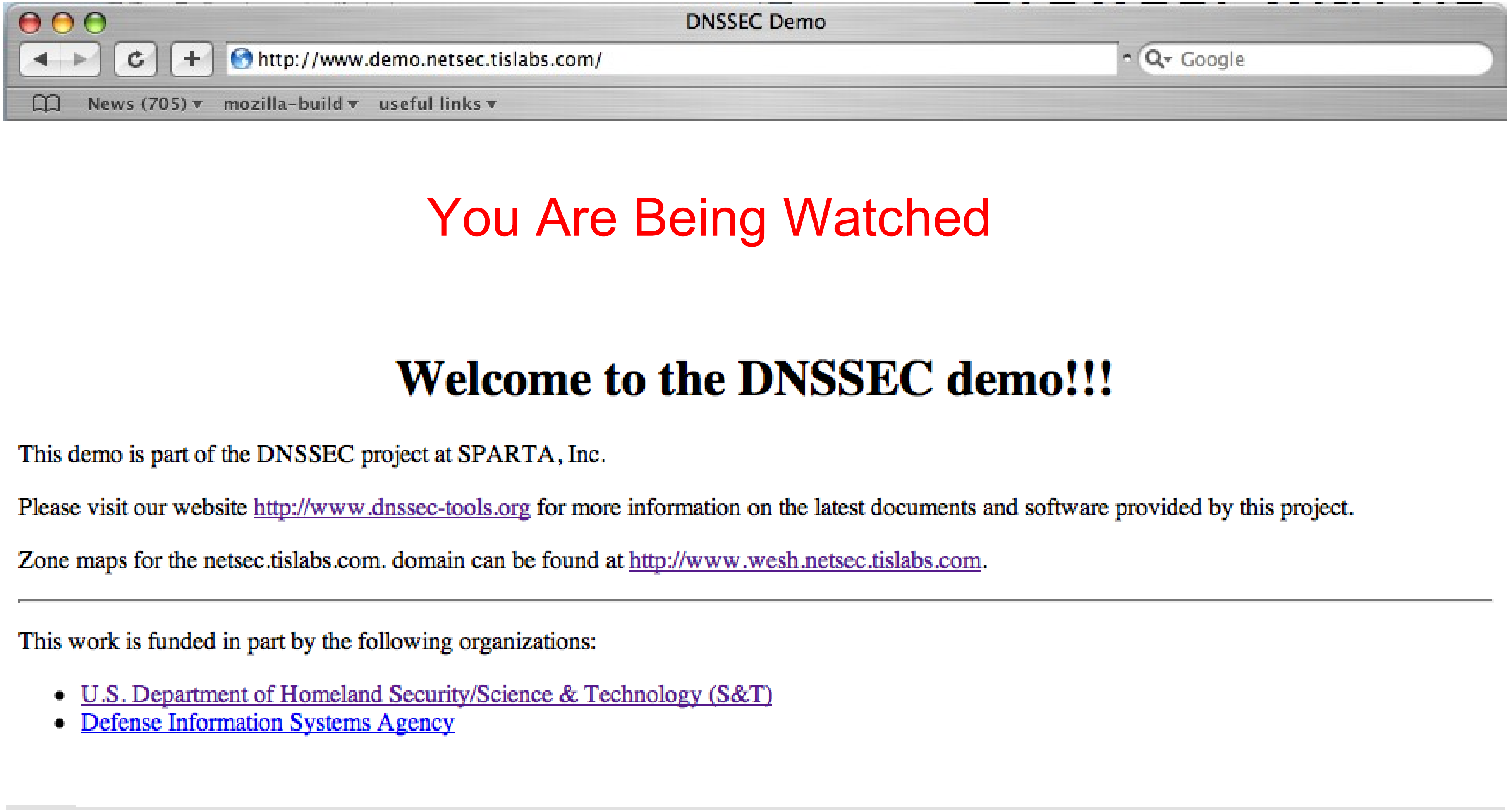


Mozilla {Build ID: 0000000000}
File Edit View Go Bookmarks Tools Window Help Debug QA
Back Forward Reload Stop
http://www.demo.netsec.tislabs.com/
Search
Print
Home Bookmarks mozilla.org mozillaZine mozdev.org
Alert
OK

www.demo.netsec.tislabs.com failed its DNSSEC security check validation. Please contact a system administrator for help.

Looking up www.demo.netsec.tislabs.com...

Browser with no DNSSEC



You Are Being Watched

Welcome to the DNSSEC demo!!!

This demo is part of the DNSSEC project at SPARTA, Inc.

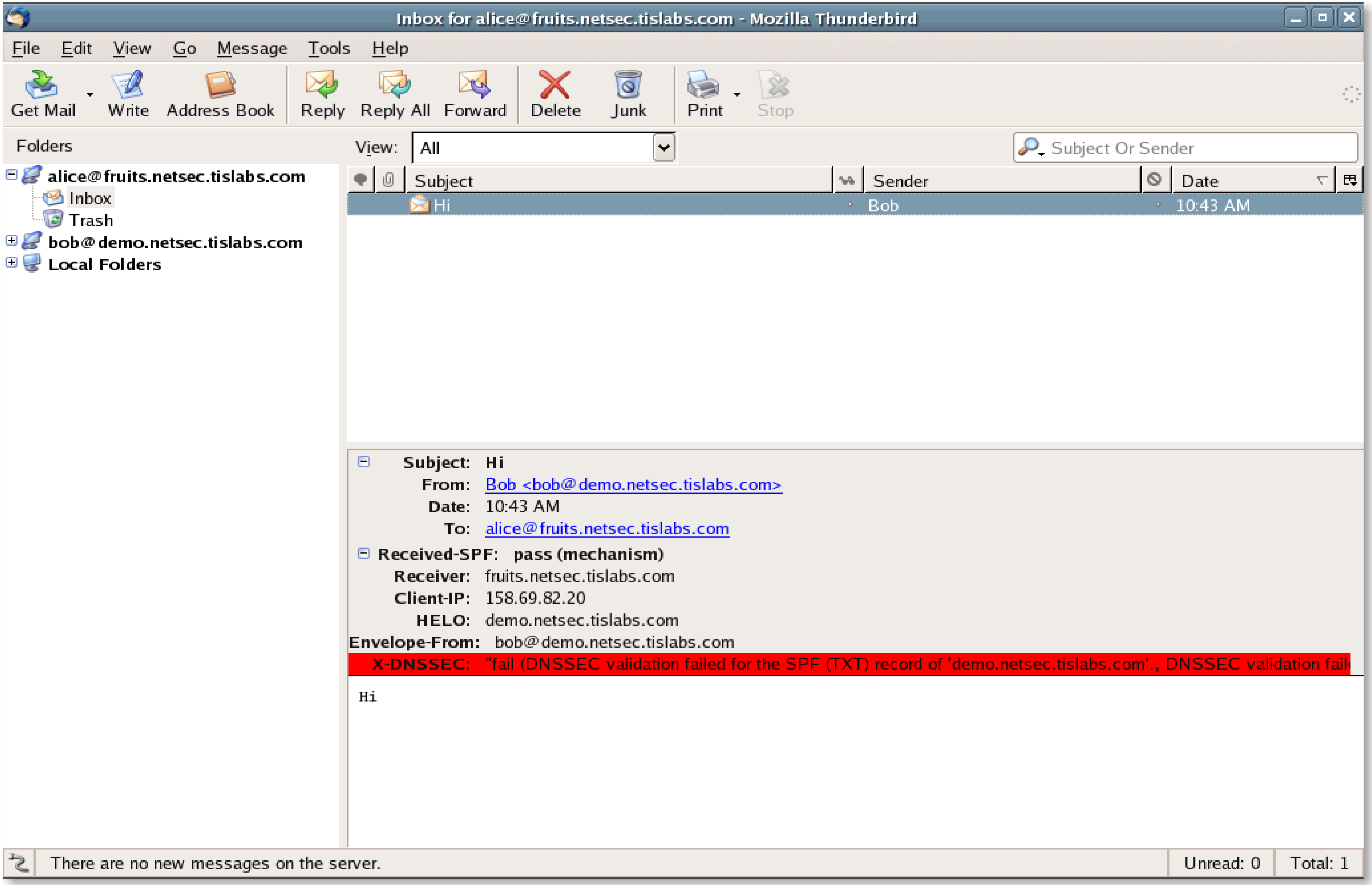
Please visit our website http://www.dnssec-tools.org for more information on the latest documents and software provided by this project.

Zone maps for the netsec.tislabs.com. domain can be found at http://www.wesh.netsec.tislabs.com.

This work is funded in part by the following organizations:

- U.S. Department of Homeland Security/Science & Technology (S&T)
- Defense Information Systems Agency

Sendmail+spfmilter detects validation failures


Inbox for alice@fruits.netsec.tislabs.com - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Mail
Write
Address Book
Reply
Reply All
Forward
Delete
Junk
Print
Stop
Folders
View: All
Subject Or Sender
alice@fruits.netsec.tislabs.com
Inbox
Trash
bob@demo.netsec.tislabs.com
Local Folders
Subject
Sender
Date

Hi Bob 10:43 AM

Subject: Hi
From: Bob <bob@demo.netsec.tislabs.com>
Date: 10:43 AM
To: alice@fruits.netsec.tislabs.com

Received-SPF: pass (mechanism)
Receiver: fruits.netsec.tislabs.com
Client-IP: 158.69.82.20
HELO: demo.netsec.tislabs.com
Envelope-From: bob@demo.netsec.tislabs.com
X-DNSSEC: "fail (DNSSEC validation failed for the SPF (TXT) record of 'demo.netsec.tislabs.com'., DNSSEC validation fail

```
Hi
```

There are no new messages on the server. Unread: 0 Total: 1

Other Tools

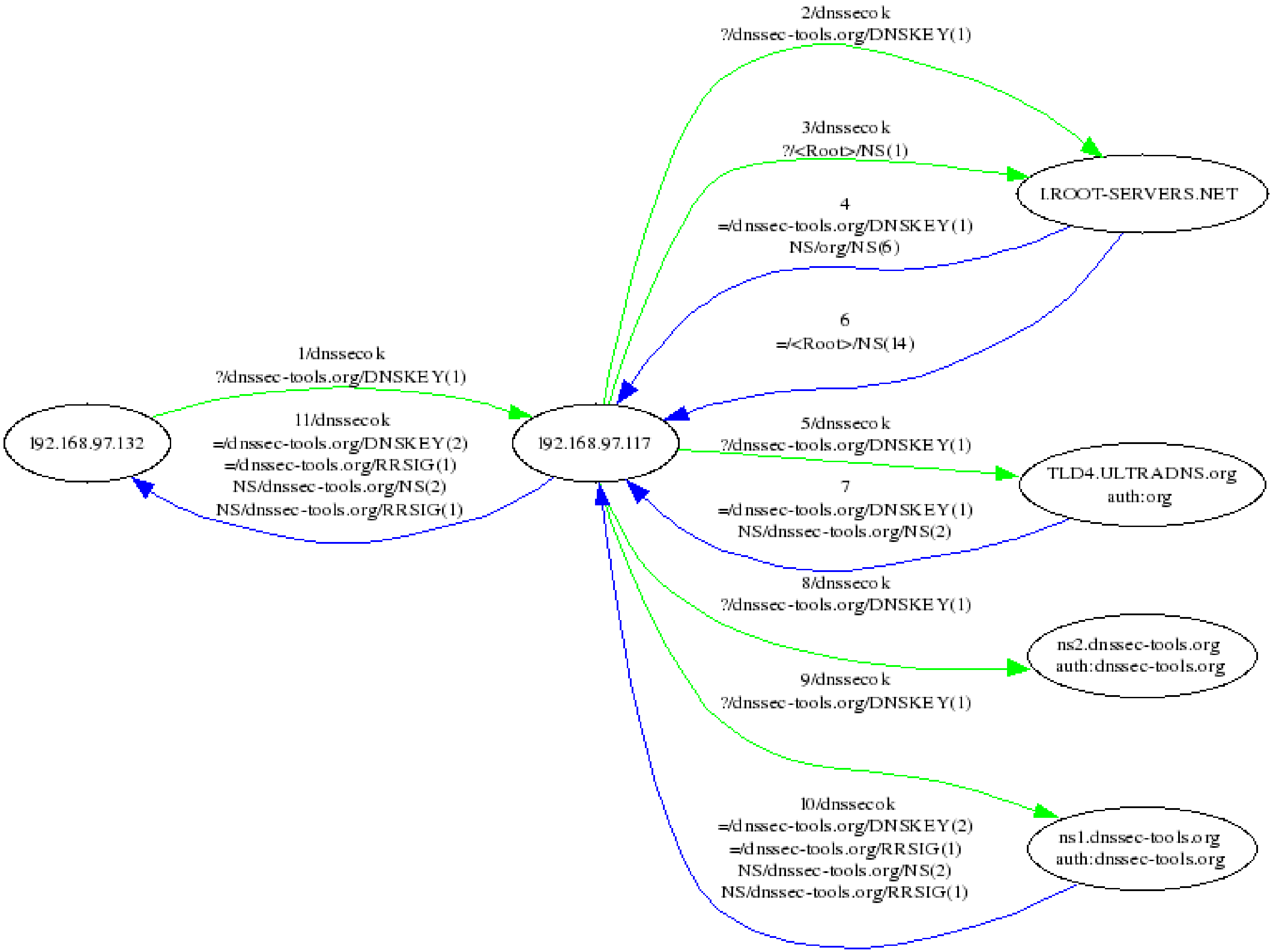
Check Your Zonefile: DoNutS

```
# donuts --level 8 -v example.com.signed example.com

--- loading rule file /usr/share/donuts/rules/dnssec.rules.txt
    rules: DNSSEC_RRSIG_TTL_MATCH_ORGTTL DNSSEC_MEMORIZE_NS_RECORDS DNSSEC_MISSING_NSEC_RECORD
DNSSEC_MISSING_RRSIG_RECORD DNSSEC_RRSIG_NOT_SIGNING_RRSIG DNSSEC_RRSIG_FOR_NS_GLUE_RECORD
DNSSEC_NSEC_FOR_NS_GLUE_RECORD DNSSEC_RRSIG_SIGEXP DNSSEC_NSEC_TTL
DNSSEC_DNSKEY_MUST_HAVE_SAME_NAME DNSSEC_DNSKEY_PROTOCOL_MUST_BE_3 DNSSEC_BOGUS_NS_MEMORIZE
DNSSEC_MISSING_RRSIG_RECORD DNSSEC_RRSIG_TTL_MUST_MATCH_RECORD DNSSEC_MISSING_NSEC_RECORD
DNSSEC_RRSIG_SIGNER_NAME_MATCHES DNSSEC_NSEC_RRSEC_MUST_NOT_BE_ALONE
DNSSEC_RRSIGS_MUST_NOT_BE_SIGNED DNSSEC_MEMORIZE_KEYS DNSSEC_RRSIGS_VERIFY
--- loading rule file /usr/share/donuts/rules/parent_child.rules.txt
    rules: DNS_MULTIPLE_NS DNSSEC_SUB_NOT_SECURE DNSSEC_DNSKEY_PARENT_HAS_VALID_DS
DNSSEC_DS_CHILD_HAS_MATCHING_DNSKEY
--- loading rule file /usr/share/donuts/rules/parent_child_temp.txt
    rules: DNSSEC_SUB_NS_MISMATCH
--- loading rule file /usr/share/donuts/rules/recommendations.rules.txt
    rules: DNS_REASONABLE_TTLS DNS_SOA_REQUIRED DNS_NO_DOMAIN_MX_RECORDS
--- Analyzing individual records in example.com.signed
--- Analyzing records for each name in example.com.signed
example.com:
  Rule Name:   DNS_NO_DOMAIN_MX_RECORDS
  Level:       8
  Warning:     At least one MX record for example.com is suggested

sub2.example.com:
  Rule Name:   DNSSEC_SUB_NOT_SECURE
  Level:       3
  Error:       sub-domain sub2.example.com is not securely delegated.  It
                       is missing a DS record.

results on testing example.com.signed:
  rules considered:           28
  rules tested:               25
  records analyzed:           52
  names analyzed:             8
  errors found:               2
```

Check your logfiles: Logwatch

```
################### LogWatch 6.0.2 (04/25/05) ####################
        Processing Initiated: Thu Jul  7 10:13:34 2005
        Date Range Processed: all
      Detail Level of Output: 10
              Type of Output: unformatted
           Logfiles for Host: host.example.com
 ##################################################################

--------------------- DNSSEC Begin ------------------------

No Valid Signature received 6 times

Detail >= 5 log messages:
   Marking as secure 97 times
   Verified rdataset succeeded 97 times
   Attempted positive response validation 96 times
   Nonexistence proof found 20 times
   Attempted negative response validation 18 times
   Validation OK 2 times

---------------------- DNSSEC End ------------------------


--------------------- Resolver Begin ------------------------


   Received validation completion event  171 times
   Validation OK  125 times
   Nonexistence validation OK received  46 times

---------------------- Resolver End -------------------------

###################### LogWatch End #########################
```

Trace your queries: dnspktFlow


2/dnssecok
?/dnssec-tools.org/DNSKEY(1)
3/dnssecok
?/<Root>/NS(1)
I.ROOT-SERVERS.NET
4
=/dnssec-tools.org/DNSKEY(1)
NS/org/NS(6)
6
=/<Root>/NS(14)
1/dnssecok
?/dnssec-tools.org/DNSKEY(1)
11/dnssecok
=/dnssec-tools.org/DNSKEY(2)
=/dnssec-tools.org/RRSIG(1)
NS/dnssec-tools.org/NS(2)
NS/dnssec-tools.org/RRSIG(1)
192.168.97.132
192.168.97.117
5/dnssecok
?/dnssec-tools.org/DNSKEY(1)
TLD4.ULTRADNS.org
auth:org
7
=/dnssec-tools.org/DNSKEY(1)
NS/dnssec-tools.org/NS(2)
8/dnssecok
?/dnssec-tools.org/DNSKEY(1)
ns2.dnssec-tools.org
auth:dnssec-tools.org
9/dnssecok
?/dnssec-tools.org/DNSKEY(1)
10/dnssecok
=/dnssec-tools.org/DNSKEY(2)
=/dnssec-tools.org/RRSIG(1)
NS/dnssec-tools.org/NS(2)
NS/dnssec-tools.org/RRSIG(1)
ns1.dnssec-tools.org
auth:dnssec-tools.org

Developer Resources

- Test zone test.dnssec-tools.org released in late December
- Validator API to be published
- Developers guide to using the validator and resolver libraries - work in progress

Documentation

- Step-by-step guide for DNSSEC operation using DNSSEC-Tools
- Step-by-step guide for DNSSEC operation using BIND tools
- Manual pages and consolidated SUM (Software User Manual)