



DNS and DNSSEC

Samuel Weiler
weiler@tislabs.com

SPARTA, Inc.
7110 Samuel Morse Dr.
Columbia, MD



Who Are We?

- SPARTA's Network Security Research group
 - Formerly Network Associates (NAI/McAfee) Labs
 - Earlier, Trusted Information Systems (TIS Labs)
- Specialize in Infrastructure Survivability
 - Routing
 - DNS
 - Network Management
- Funded by DHS, et. al.



Credits

- My colleagues
 - Russ Mundy
 - Wes Hardarker
 - Suresh Krishnaswamy
 - Wes Griffin
 - Abhijit Hayatnagarkar
 - Wayne Morrison
 - Lindy Foster
- Olaf Kolkman
 - NL Net Labs, IETF DNSEXT WG chair



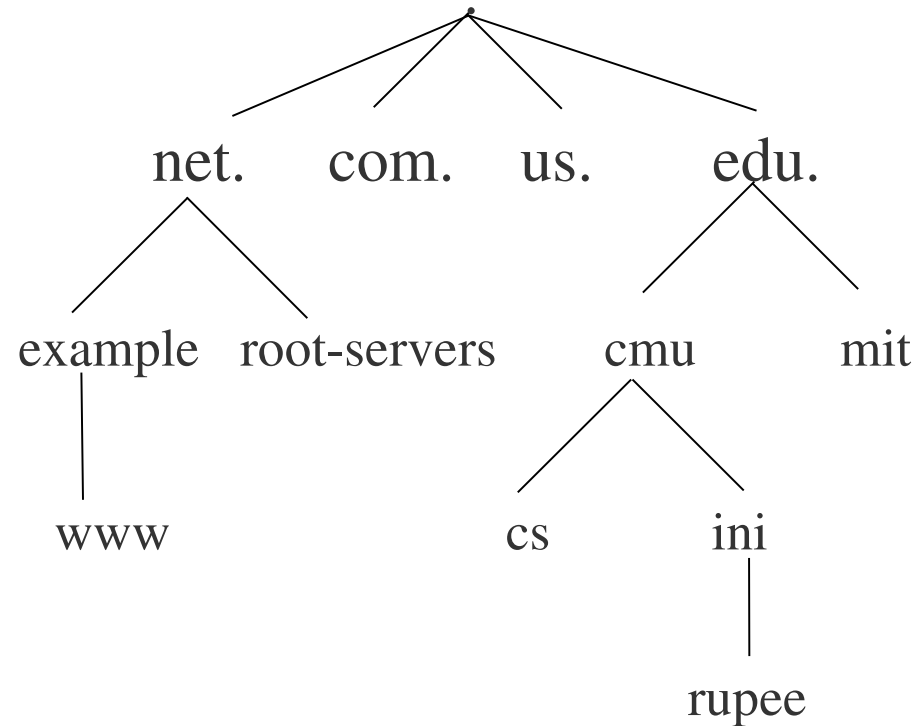
Outline

- Intro to DNS
 - Threats and vulnerabilities
- DNSSEC
 - Design Principles
 - Mechanics
 - State of Implementation
 - Applications & Tools
 - Historical perspective: design challenges
- Questions



Domain Name System (DNS)

- A globally distributed, loosely coherent, scalable, reliable, dynamic, hierarchical database
- Unique global root
- Every domain name may have multiple resource record sets (RRsets)



cmu.edu MX 10 cmu-mx1.andrew.cmu.edu

cmu.edu MX 20 cmu-mx2.andrew.cmu.edu

cmu.edu A 128.2.11.43



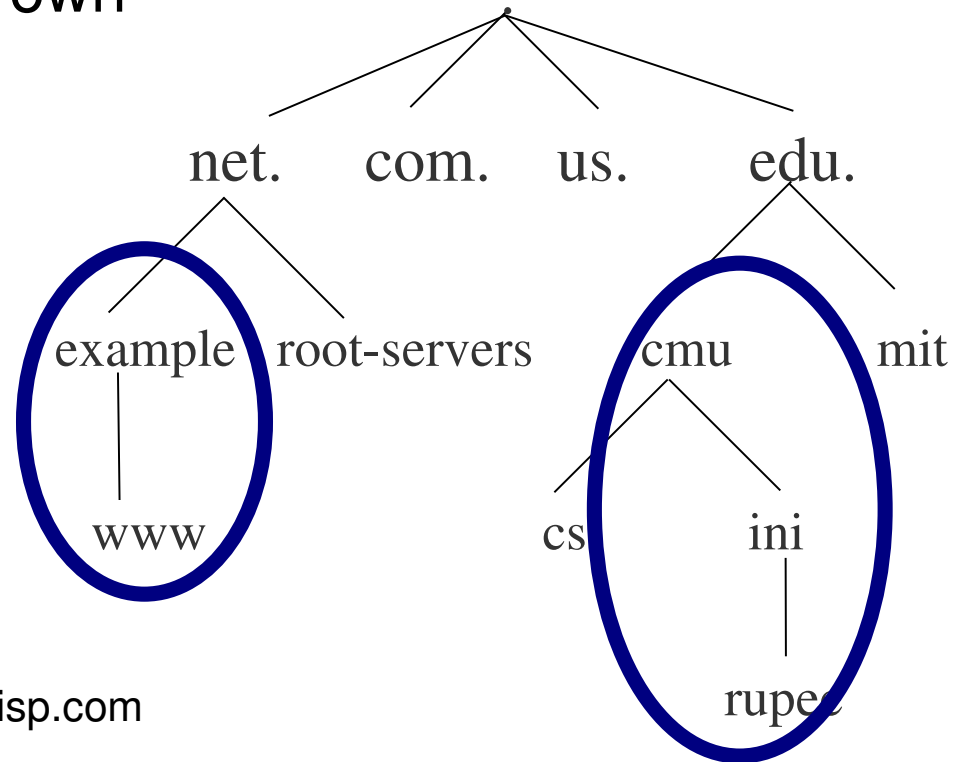
Zones and Delegations

Hierarchy is broken into *zones*

Each zone is authoritative for its own data

At a delegation, the parent zone contains a nameserver (NS) RRset for the child

The child zone may have other RRsets, also



In net. (the parent): example.net NS ns1.isp.com

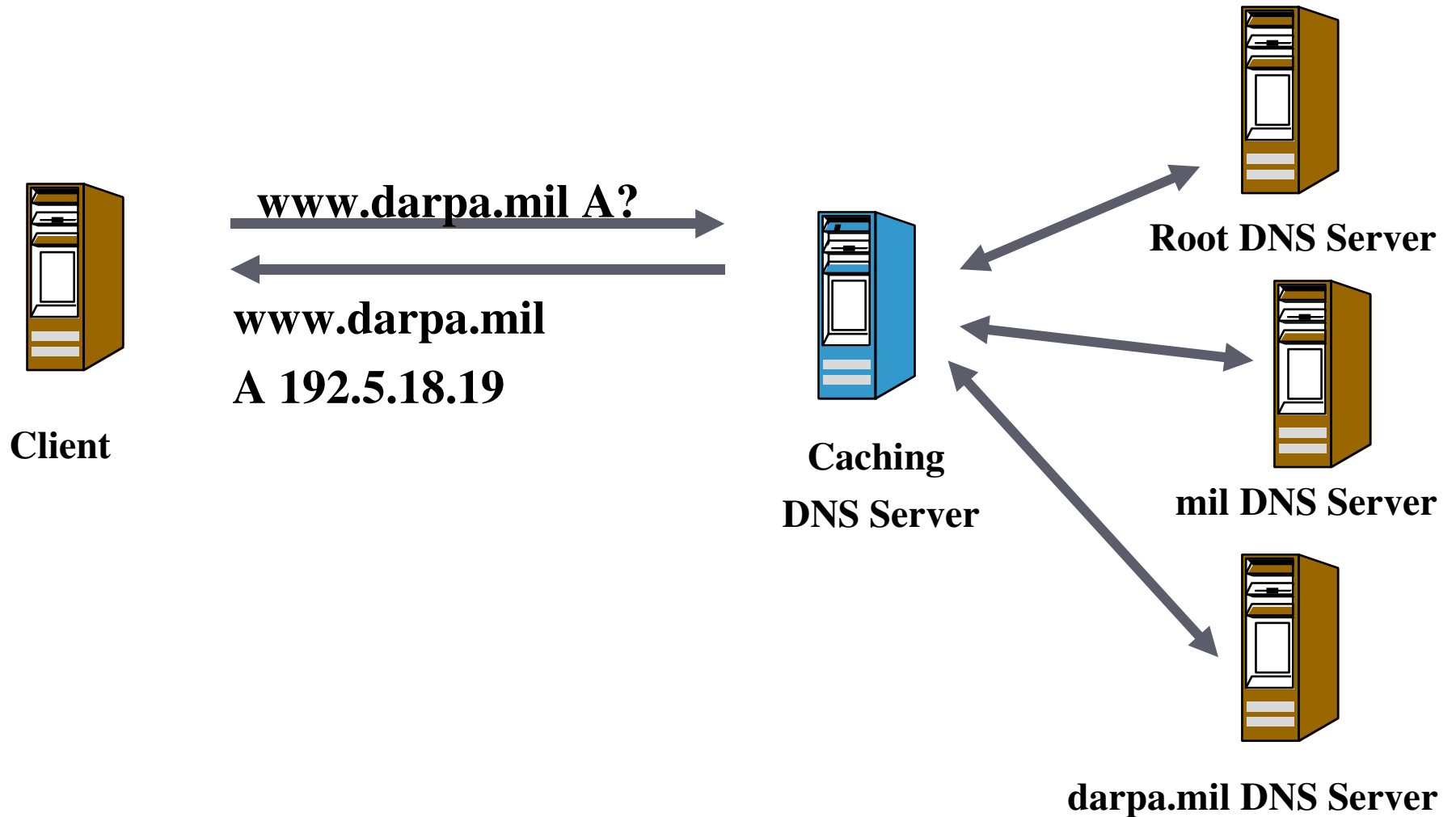
In example.net. (child): example.net NS ns1.isp.com

 A 192.169.3.4

 MX 10 mail.isp.com

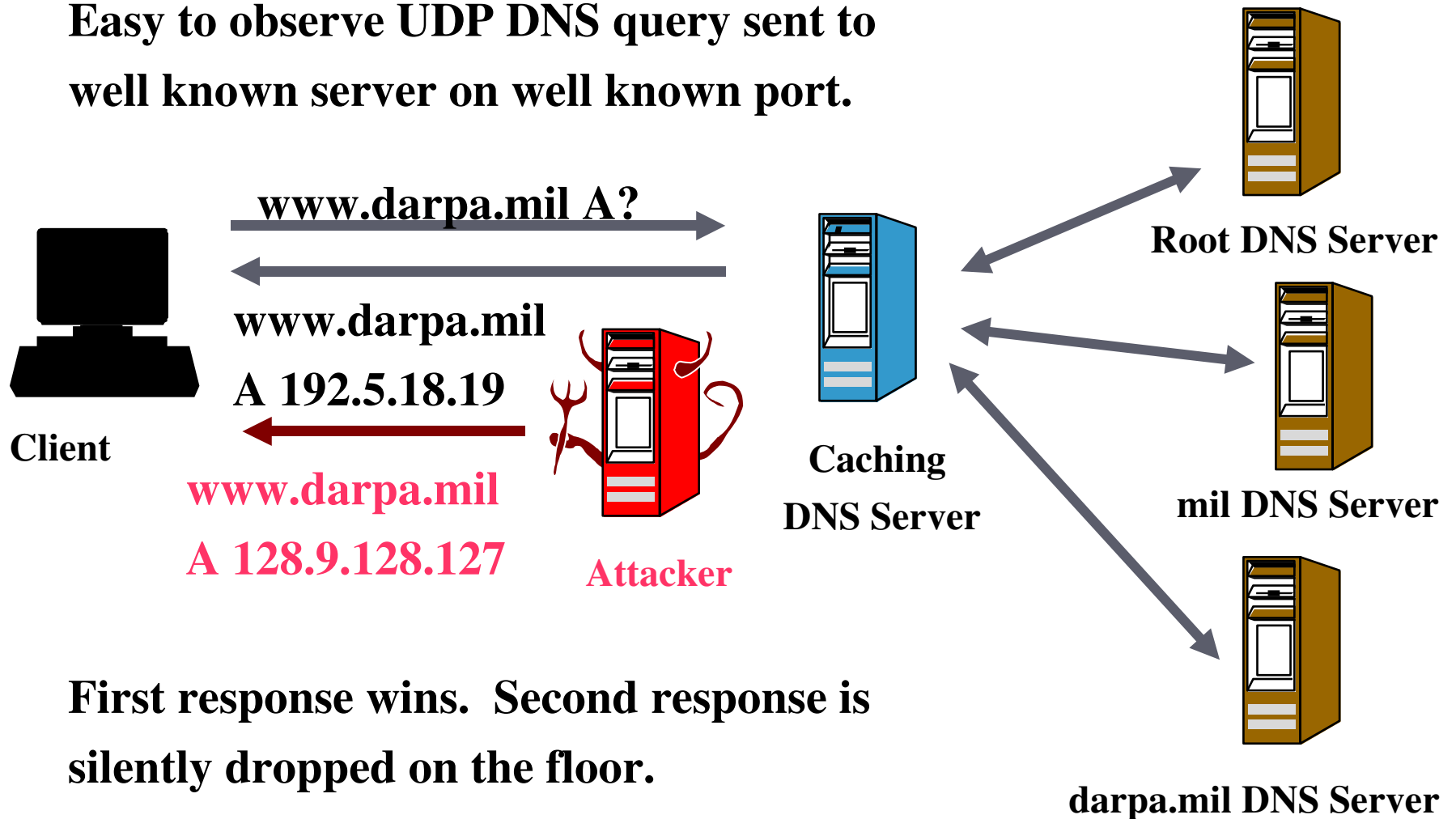


DNS Resolution



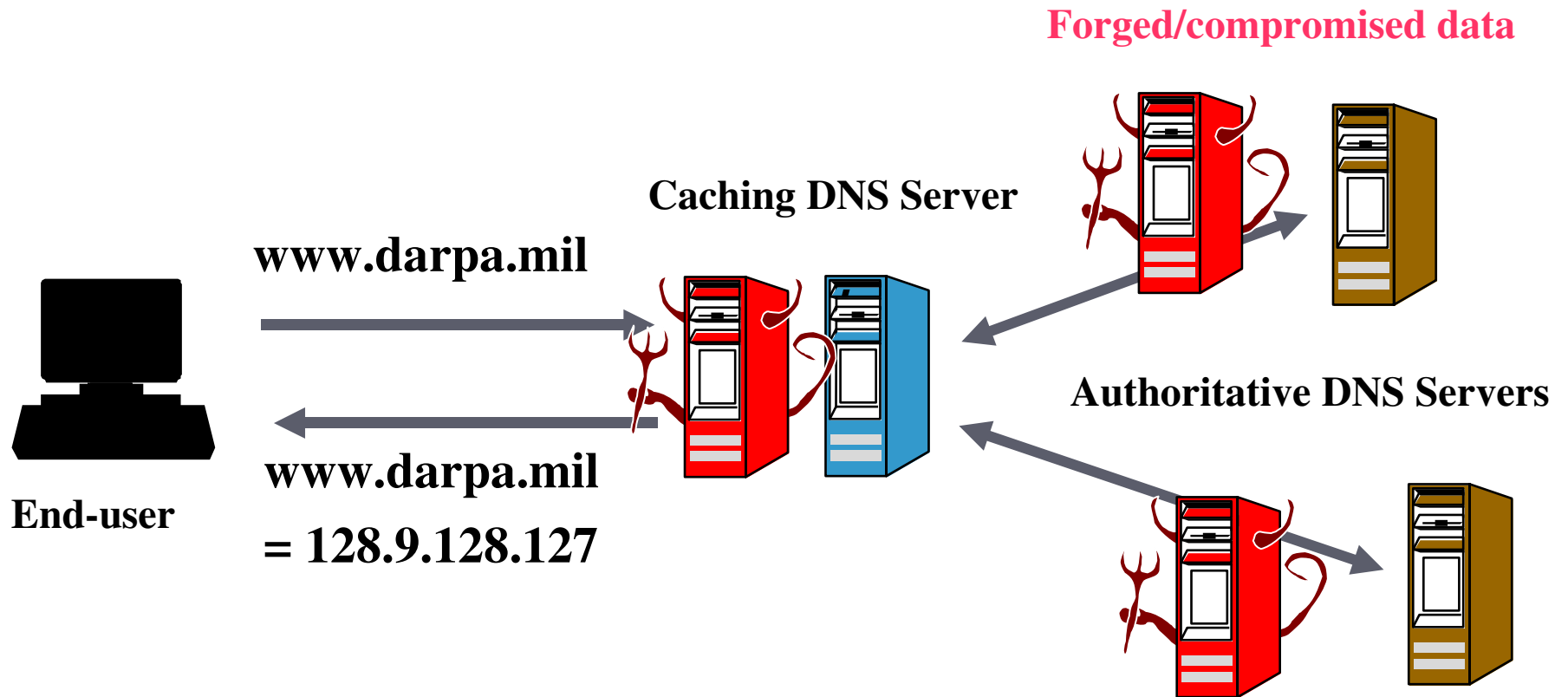
A Simple DNS Attack

Easy to observe UDP DNS query sent to well known server on well known port.



First response wins. Second response is silently dropped on the floor.

DNS Vulnerabilities



Actually www.darpa.mil = 192.5.18.195.

But how do you determine this?



What's at Stake?

- DNS attacks are often a precursor to other attacks
- Forged DNS data breaks critical applications
 - Web site can be replaced with a false site without ever touching the victim site
 - E-mail can be re-routed or mis-delivered
 - Insert a man-in-the-middle
- Can be difficult to counter the attack at the application level
 - Typically no alternative if DNS fails
- DNS attack tools readily available on the Internet, e.g., dsniff, dnshijack



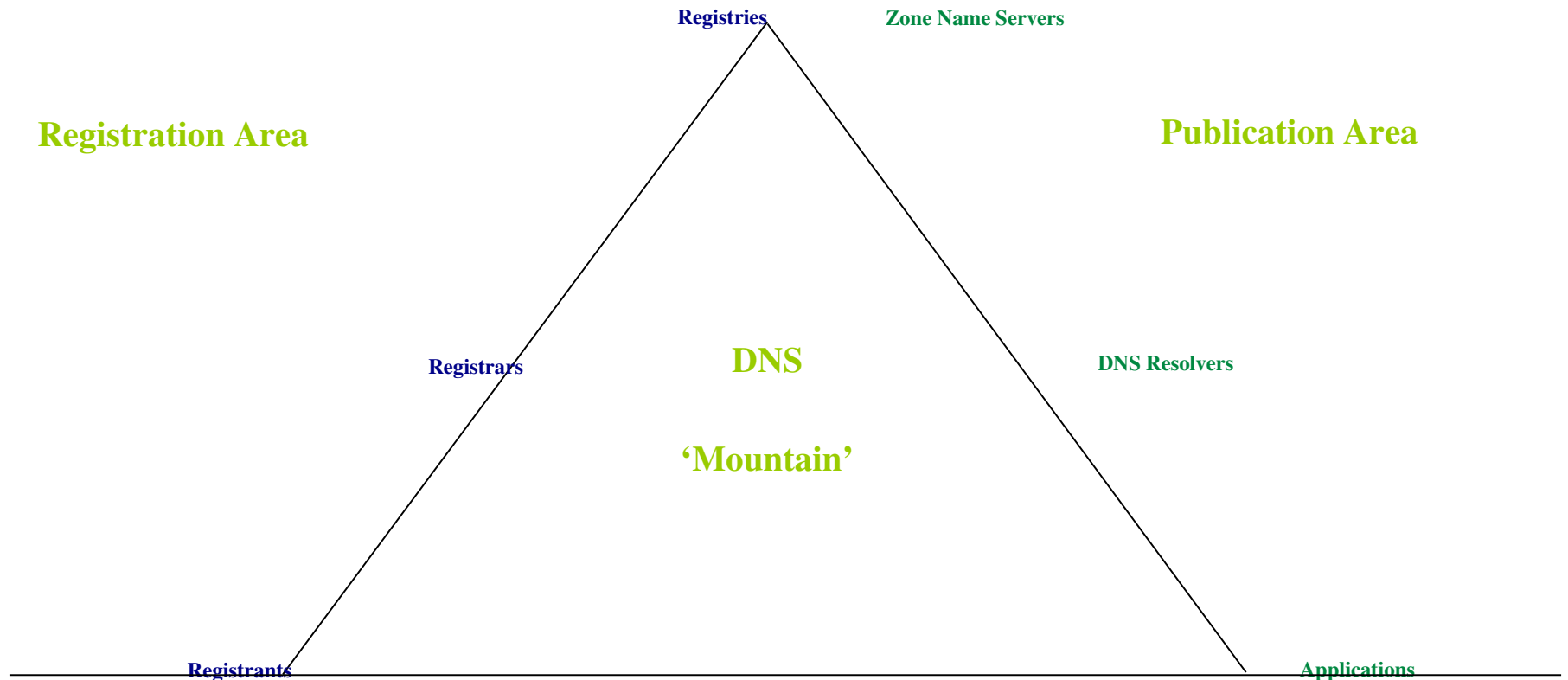
DNSSEC Scope

- Provide data source authentication and integrity protection
- Protect against data forgery and cache poisoning
- May mitigate risk of DNS server compromise IF private keys are held off-line

- No DoS/DDoS protection
- No confidentiality
- No revocation mechanism
 - Relies on short “certificate” lifetimes

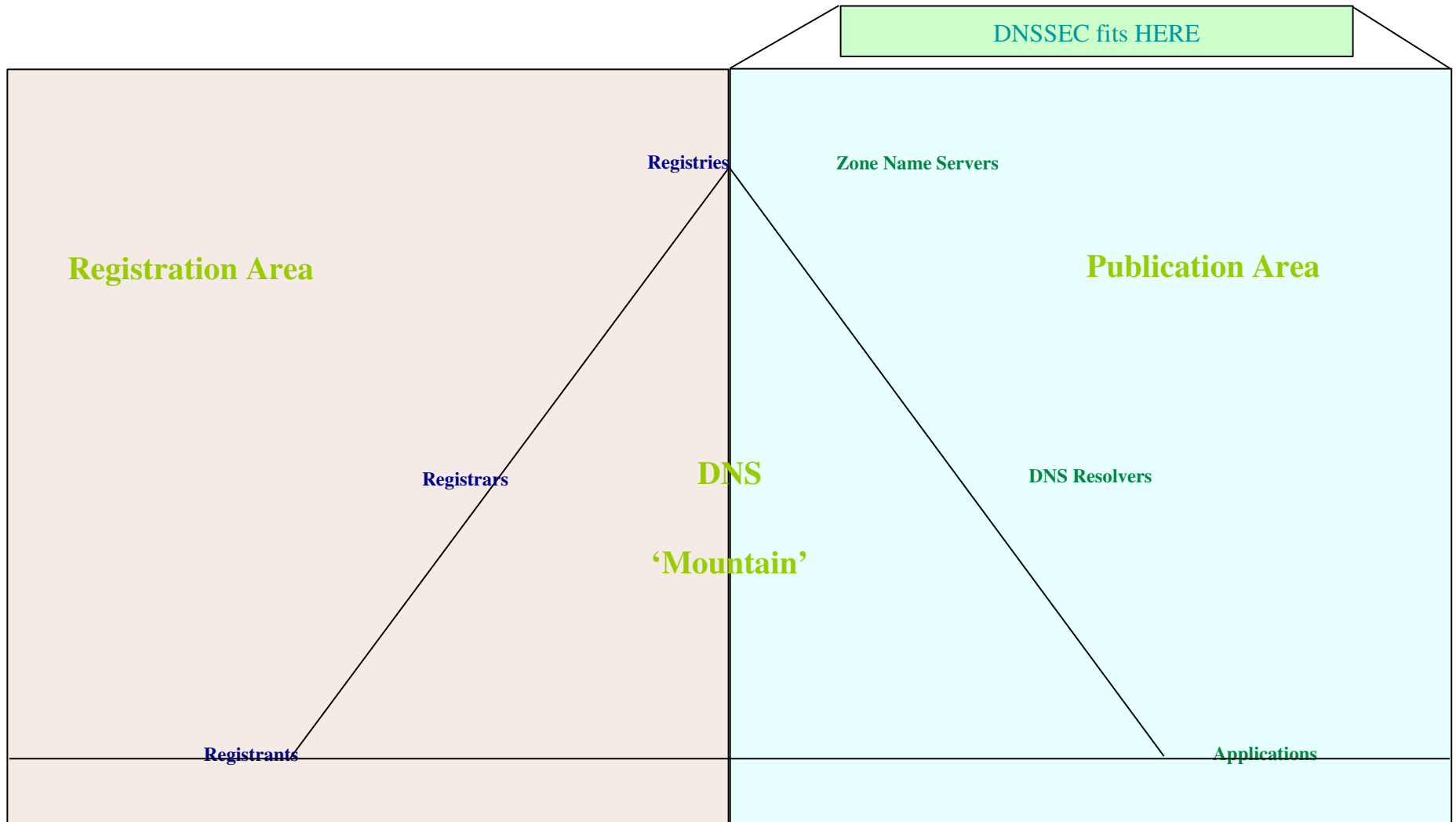


Where Does DNSSEC Fit?





Where Does DNSSEC Fit? (cont.)





DNSSEC Design Principles

- Stay in-band
- New capabilities must not disrupt old implementations
- Authenticate DATA, not QUERIES
 - TSIG and SIG(0) to protect queries and updates
- Allow off-line storage of signing keys
 - No crypto-on-demand
 - Secondary authoritative servers don't need keys
- Start with a *trust anchor* for a high level zone (e.g. the root)
 - No pairwise keying
- “Certificate” chain authenticates keys of each zone in the delegation chain
- Use “certificate” lifetimes; no explicit CRLs; no CRL checking



Who Must Do What

- Registries & registrars
 - Provision to accept keying material
- Zone operators (& registries)
 - New software (built into current BIND and NSD)
 - Ongoing key management & resigning
- End hosts & resolvers
 - Optional new software
 - Trust anchor management



DNSSEC Mechanics Outline

- New RRs
 - DNSKEY
 - RRSIG (Resource Record SIGNature)
 - DS (Delegation Signer)
- Authentication Chains
- More new RRs
 - NSEC (Next SECure)
- Validation



DNSKEY Resource Record

- Stores the public half of an asymmetric key pair
- Belongs to the ZONE, not the server
- Stored at the zone apex (along with the SOA, NS, A?, MX?)
- May have multiple DNSKEYs per zone
- Example

```
example.net 3600 IN DNSKEY 256 3 3 AJXxPAbJ+2eDT88mcWRc2fjrio/Ho
```



RRSIG Resource Record

- Public key signature on one authoritative RRset made with one DNSKEY
- Authenticates that RRset
- Limited validity interval
- Example

```
example.net 3600 RRSIG NS 3 2 3600 20040319180202 20040218180202 27036  
example.net. AEOAhHAPDOSKjeOR1sOYBEaDkWtk=
```

NS: RRset that this RRSIG applies to

3: Algorithm

2: Number of labels in the name signed (used to detect wildcard answers)

3600: original TTL

20040319180202: signature expiration, YYYYMMDDHHmmSS in UTC

20040218180202: signature inception

27036: key tag of the DNSKEY used to make this RRSIG

example.net: signer name



Delegation Signer (DS) RR

- Indicates which DNSKEY(s) the child may use
 - Contains a hash of that DNSKEY
- Establish an expectation that the child will be signed
- Appears at a delegation in the parent zone ONLY
- Also proves the existence of a delegation
- Example

```
example.net. 3600      IN NS      ns1.isp.com.  
example.net. 3600      IN DS      27374 599909F9B767FBD6...B758D
```



Authentication Chains

- Alternating sequence of DNSKEY and DS RRs
 - Start with a “trusted” DNSKEY
 - Preconfigured
 - Need authenticated out-of-band transfer
 - That key signs a zone's DNSKEYset, authenticating other DNSKEYs
 - Any of those DNSKEYs can sign other data in the zone
 - DS records at the parent show which DNSKEYs may sign a child's DNSKEYset
 - End at the DNSKEY that authenticates the given RR

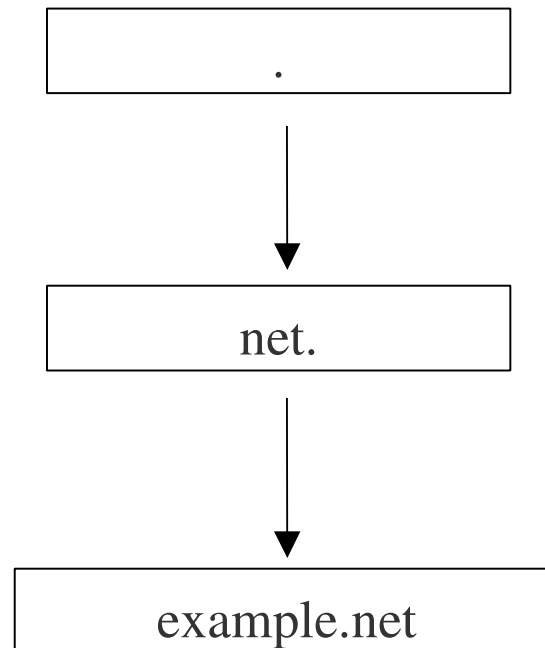


Authentication Chains Example

. DNSKEY K1
. DNSKEY K2
. RRSIG(K1) DNSKEY
net DS K3
net RRSIG(K2) DS

net DNSKEY K3
net DNSKEY K4
net RRSIG(K3) DNSKEY
example.net DS K5
example.net RRSIG(K4)

example.net DNSKEY K5
example.net DNSKEY K6
example.net RRSIG(K5) DNSKEY
example.net SOA
example.net RRSIG(K6) SOA



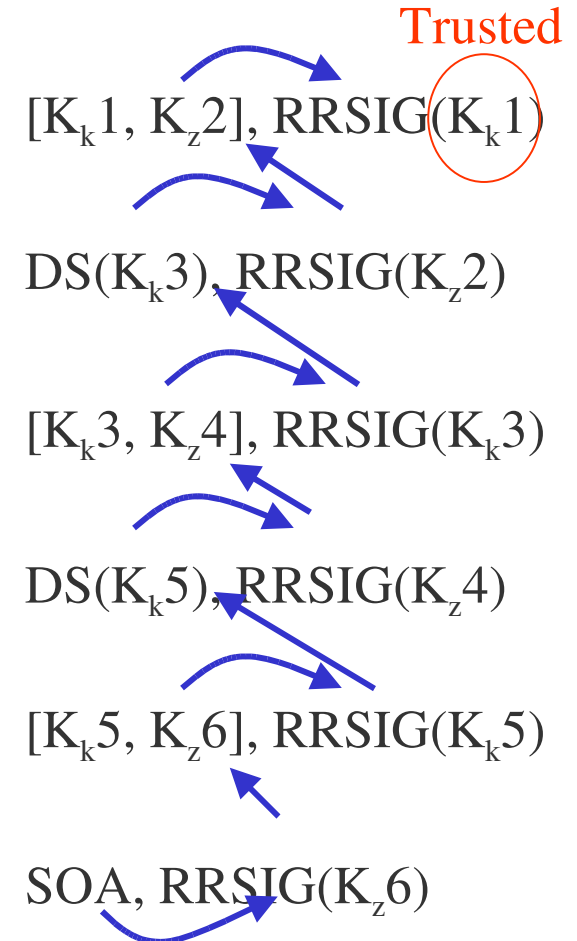
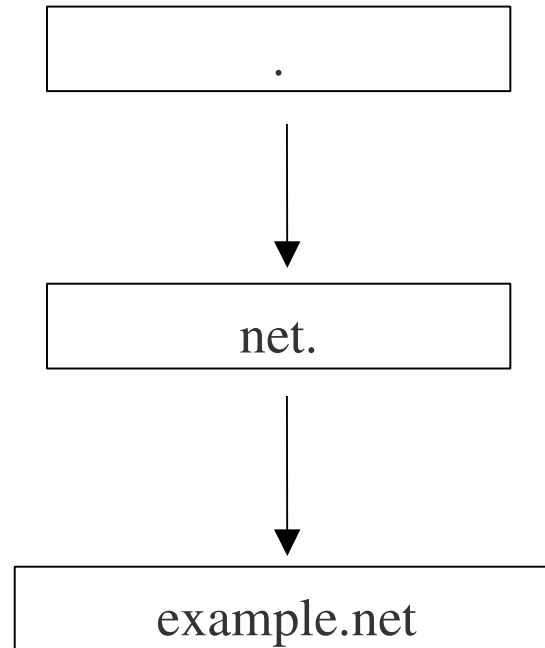


Authentication Chains Example

. DNSKEY K1
. DNSKEY K2
. RRSIG(K1) DNSKEY
net DS K3
net RRSIG(K2) DS

net DNSKEY K3
net DNSKEY K4
net RRSIG(K3) DNSKEY
example.net DS K5
example.net RRSIG(K4)

example.net DNSKEY K5
example.net DNSKEY K6
example.net RRSIG(K5) DNSKEY
example.net SOA
example.net RRSIG(K6) SOA





Next SECure (NSEC) RR

- Proves what data is (and isn't) in the zone
 - Lists the RR types present at a name
- Example
 - a.example.net. 3600 NSEC b.example.net. NS RRSIG NSEC
- Identifies the next name in the (sorted) zone
 - NSEC for the last name points to the SOA
 - z.example.net. 3600 NSEC example.net. NS RRSIG NSEC SOA DNSKEY
- Sent with
 - NXDOMAIN answers
 - Unsecure delegations (to prove that there's no DS)



NSEC3 RR

- Confidentiality of zone contents had been a non-requirement
 - Now a requirement for some zone
- Optional replacement for NSEC
- Still proves what data is (and isn't) in the zone
 - Still lists the RR types present at a name
- NEW: hashes all names in the zone and sorts based on those hashes
- Example

```
0dasdk3qdk3kdoakfocoaskwodkcowksik.example.net. 3600 NSEC3  
( 0 1 0 weaksalt fhghjvicxkiokcklcoiwocxklsdioecncfnsi A MX )
```



Validation Results

- Having a preconfigured *trust anchor* establishes the expectation that data below that point will be signed
- Possible results
 - SECURE: there is a valid chain of DNSKEYs, RRSIGs, and maybe DSs down to the data
 - UNSECURE (default): there's no applicable preconfigured trust anchor OR there is a SECURE path to a delegation with an NSEC proving that no DS exists (an unsecure delegation)
 - BOGUS: expected SECURE data wasn't there
- Handling of result up to resolver or application



State of Implementation

- End-host components
 - DNS Resolver Software
 - BIND and Unbound (java), both open source
 - Applications
- Components for registries & zone operators
 - Authoritative server software
 - BIND & NSD, both open source
 - Tools
 - MANY sites, especially larger ones, generate DNS zone files from an automated system



End-host Support: Why?

- Users may need different policies from their ISPs
 - E-Mail from a client is critical
- Applications may each need different policies
 - software downloads (http, ftp)
 - email sending/receiving (smtp, pop, imap)
 - reading news (nntp)
 - time synchronization (ntp)



Why Do We Care, Part 2

- Without application level policy
 - System level policies don't allow for end user knowledge or end-user decisions.

Unknown host "www.broken.example.com"

Ok



Why Do We Care, Part 3

- With application level policy

SEVERE ERROR:

"www.broken.example.com" failed DNSSEC Validation

Continue anyway?

Yes

No

Warning: DNSSEC signature for
"www.broken.example.com" expired

Continue anyway?

Yes

No



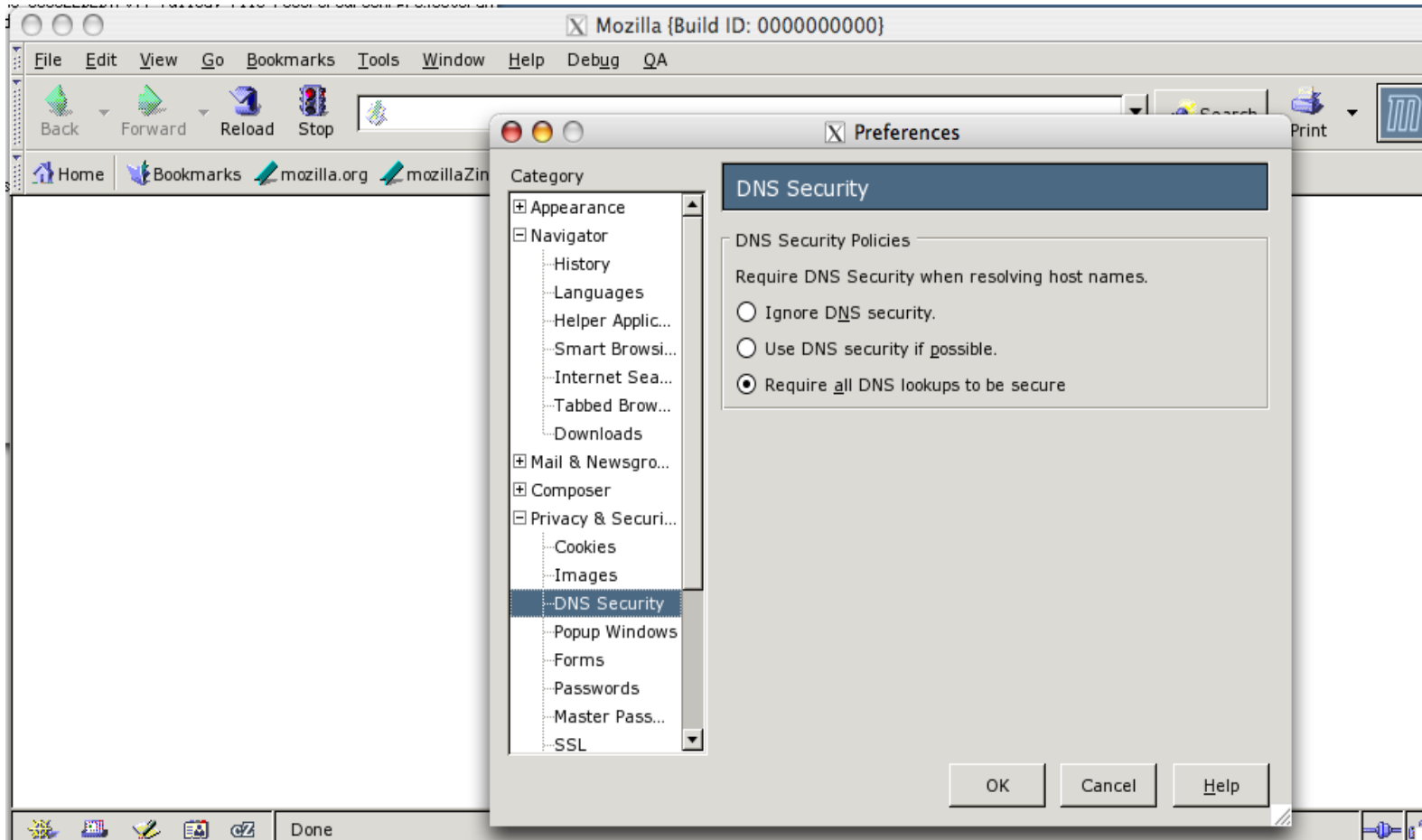
End-host Support: What's Out There?

- DNS Resolvers
 - BIND
 - Unbound (java)
 - More coming...
- Application support, from SPARTA's DNSSEC-tools project
 - Sendmail/postfix patch to validate SPF records and other DNS lookups
 - Email client extension to show validation results
 - Web browser plugin to do validation



DNSSEC-aware Mozilla

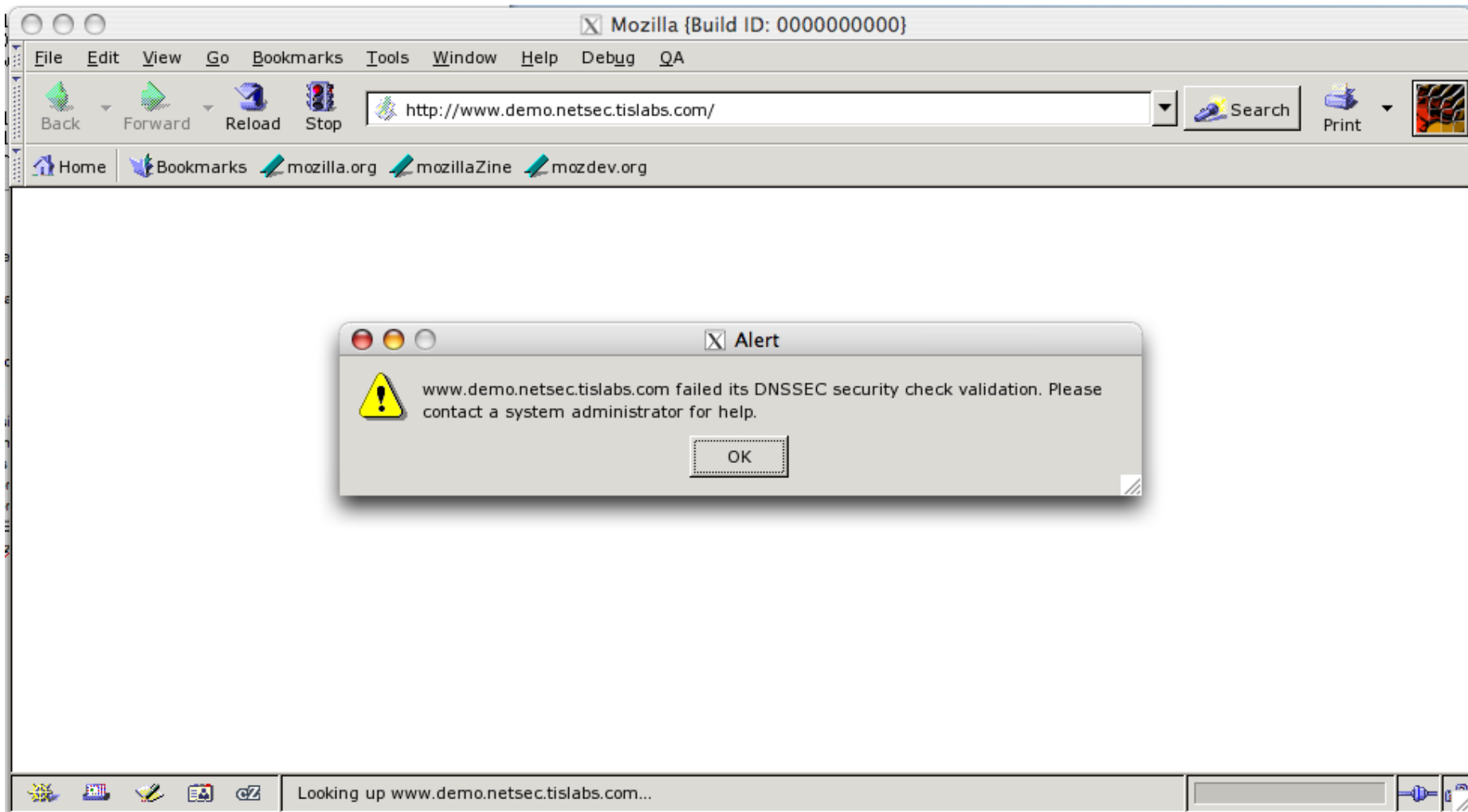
(www.dnssec-tools.org)





Mozilla detects validation failures

(www.dnssec-tools.org)





DNSSEC-aware Sendmail+spfmlite

(www.dnssec-tools.org)

The screenshot shows the Mozilla Thunderbird interface. The window title is "Inbox for alice@fruits.netsec.tislabs.com - Mozilla Thunderbird". The menu bar includes File, Edit, View, Go, Message, Tools, and Help. The toolbar contains icons for Get Mail, Write, Address Book, Reply, Reply All, Forward, Delete, Junk, Print, and Stop. The left sidebar shows folders for alice@fruits.netsec.tislabs.com (Inbox, Trash) and bob@demo.netsec.tislabs.com. The main pane shows a list of messages with columns for Subject, Sender, and Date. The selected message has the subject "Hi" and is from Bob, dated 10:43 AM. The message details pane shows the following information:

- 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"

The message body contains the text "Hi".

At the bottom of the window, a status bar indicates "There are no new messages on the server." and shows "Unread: 0" and "Total: 1".



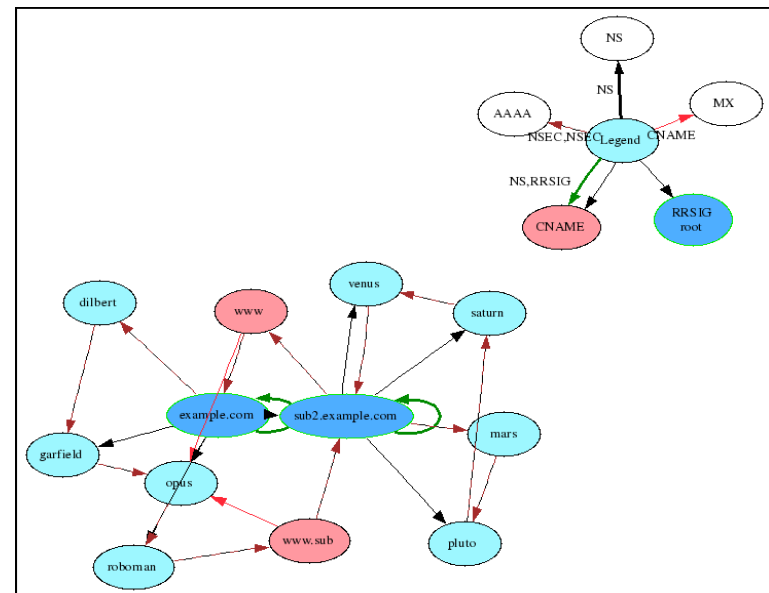
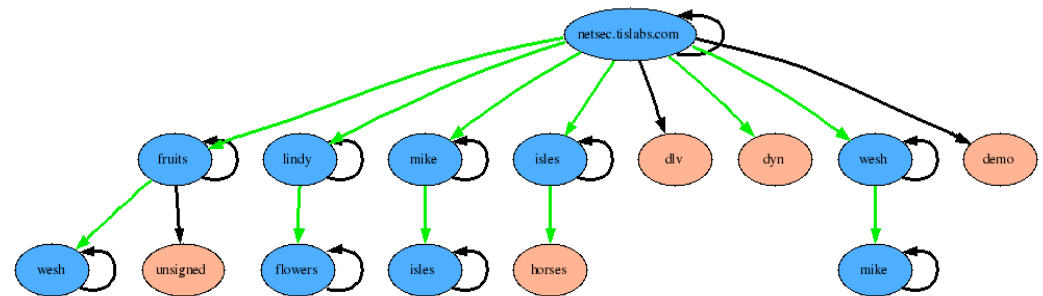
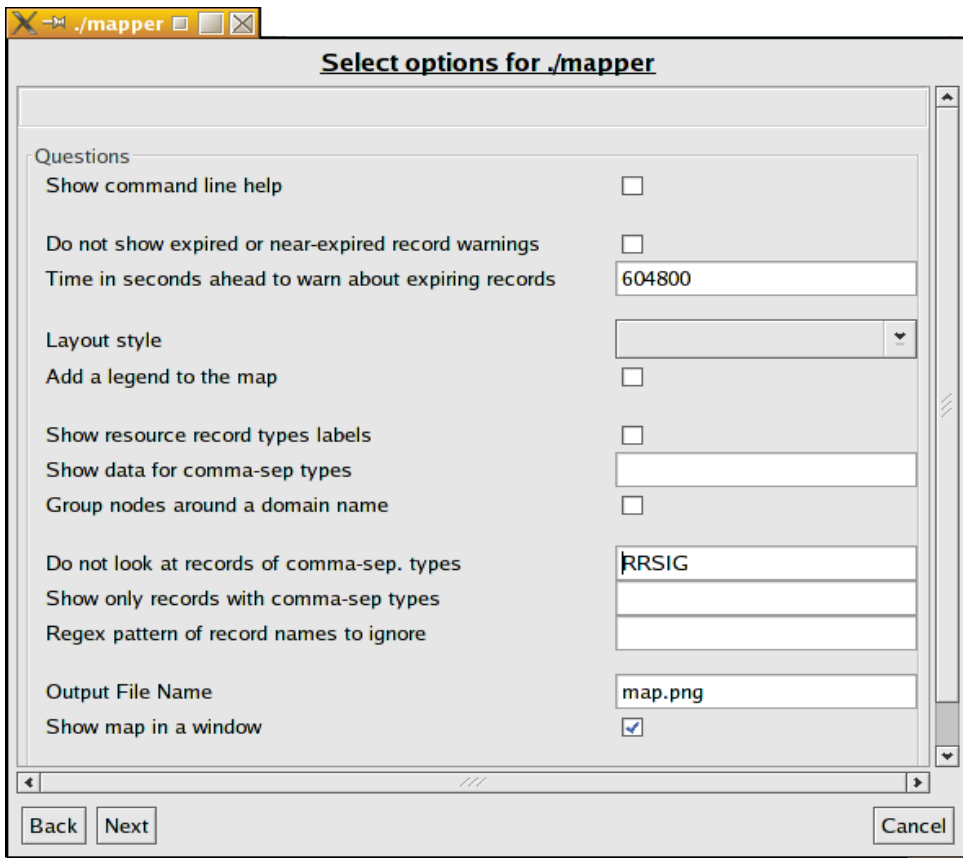
Tools

- DNSSEC-Tools (SPARTA)
 - Zone visualization
 - Zone signing tools
 - Zone error checker
 - Key maintenance
 - Log file analysis
 - Net::DNS::Sec::Tools per module
- Key maintenance tools (RIPE)
- Net::DNS::Sec perl module (Nlnet Labs)
- And many others



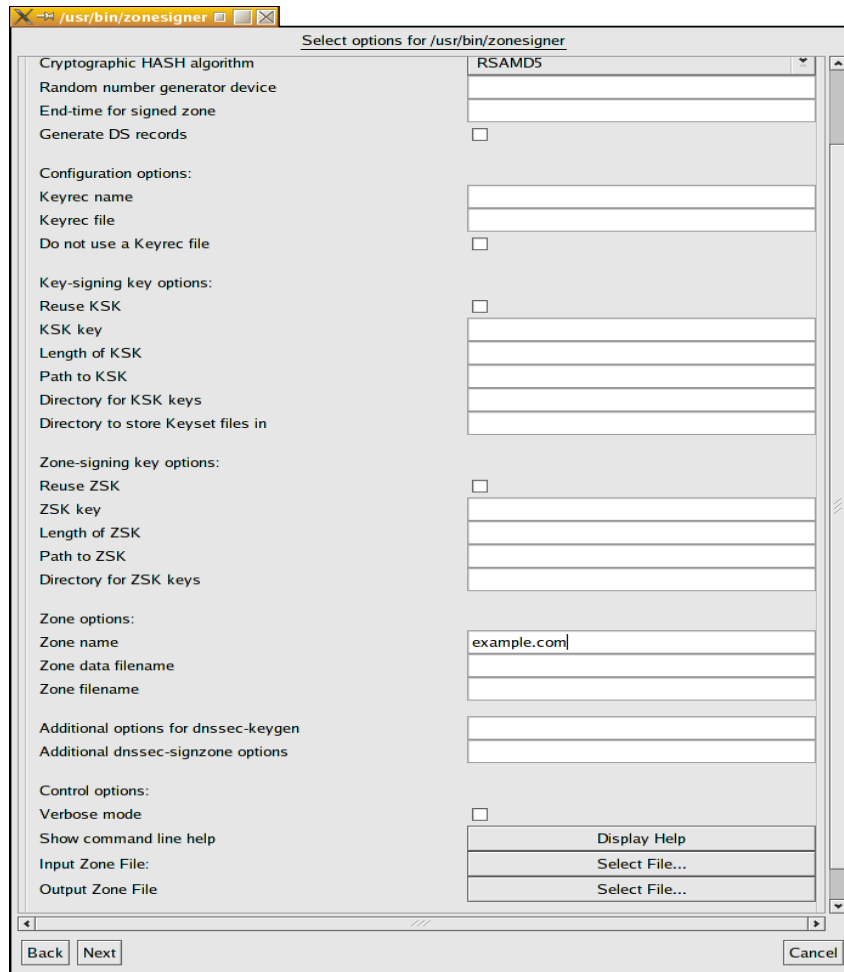
Zone visualization tool

- Quickly spot unsigned or broken delegations





Zonesigner



- Automates key generation and zone signing
- Components useful for building custom tools



Design Challenges (historical)

- RFC2535: required tight parent-child synchronization
 - New requirement in the DNS
 - Parent could NOT roll key without cooperation of all children
 - Fixed by adding a layer of indirection
 - Delegation Signer (DS)
- Delegation Signer
 - First RR to appear ONLY in the parent, not in the child
 - Protocol issues (fully resolved)
- Zone walking
 - Confidentiality had been a non-requirement
 - NSEC3 RR developed



Operational Impact

- Non-challenge: relatively EASY to sign a zone
 - May require integration into existing process
 - Requires regular resigning
- Maintaining trust anchors in resolvers/applications
 - Especially when high-level zones aren't signed
 - DNSSEC Lookaside Validation (DLV)
 - Allows “outsourcing” of trust anchor configuration
- Extra data passed between parent and child zones
- What happens on validation failure
 - Ongoing work on a validator API



Resources

- BIND: <http://www.isc.org/>
- NSD: <http://www.nlnetlabs.nl/nsd/>
- SPARTA's DNSSEC Tools (zone signer, error checker, visualization, log analysis, applications) :
<http://dnssec-tools.sourceforge.net/>
- Key maintenance tools from RIPE:
<http://www.ripe.net/projects/disi/>
- Net::DNS::Sec perl module: CPAN
- Even more: <http://www.dnssec.net/>



Questions?
