Secure DNS with Unbound and DNSSEC-Trigger

Implementation and Deployment

MEN&MICE

© Men & Mice http://menandmice,com

Agenda

- DNS Threats
- DNSSEC Introduction
- the problem of the last mile
- Unbound validating DNS Server
- DNSSEC-Trigger
- tools and troubleshooting
- deinstallation

DNS Threats

© Men & Mice http://menandmice,com

The problem with DNS

- The original DNS (designed in 1983) has no security build in
  - it is very easy to change DNS traffic “on-the-fly”
  - Bad-Guys, Companies and Governments try to use this fact for their goals

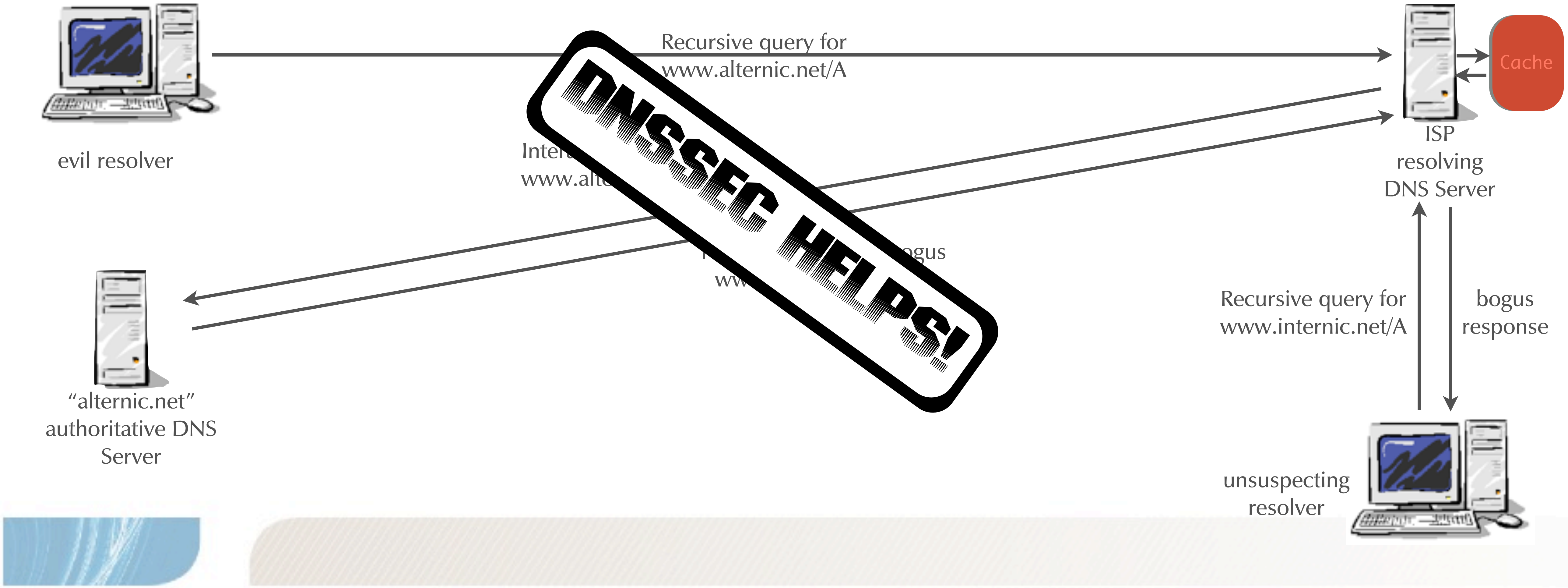
DNS Cache Spoofing
Episode I

the Kaspureff attacks
12. July 1997

MEN&MICE

The Kashpureff Attack

- In July, 1997, Eugene Kashpureff used a direct triggered cache poisoning attack against the InterNIC's web site



© Men & Mice http://menandmice,com

DNS 'bailiwick' checking

- The problem:
    - The Kashpureff attack has been possible because DNS Servers were accepting arbitrary information from the additional section of the DNS answer

DNS 'bailiwick' checking

- The fix
  - The credibility checking when replacing cache entries
  - Check for "in bailiwick" in response data. Answer records must be from the same domain as the requested name.

Data not in 'bailiwick' will not be accepted

```
$ dig @ns1.example.com www.example.com
;; ANSWER SECTION:
www.example.com.    120      IN    A    192.0.2.10

;; AUTHORITY SECTION:
example.com.   86400    IN    NS   ns1.example.com.
example.com.   86400    IN    NS   ns2.example.com.

;; ADDITIONAL SECTION:
ns1.example.com.    604800   IN    A    192.0.2.120
ns2.example.com.    604800   IN    A    192.0.2.130
~~www.mybank.com.    604800   IN    A    1.2.3.4~~
```

© Men & Mice http://menandmice,com

DNS Cache Spoofing
Episode II

the Amit Klein findings
March-June 2007

MEN&MICE

Message ID Guessing

- The DNS message’s message ID field is only 16 bits long
    - And the "randomizer" of some nameservers is not truly random
        - It’s worse in BIND before 8.2
        - Though it’s better in BIND 8.2 and later versions with use-id-pool set and in versions of BIND 9
        - It is only real random in BIND version from end of 2007 on

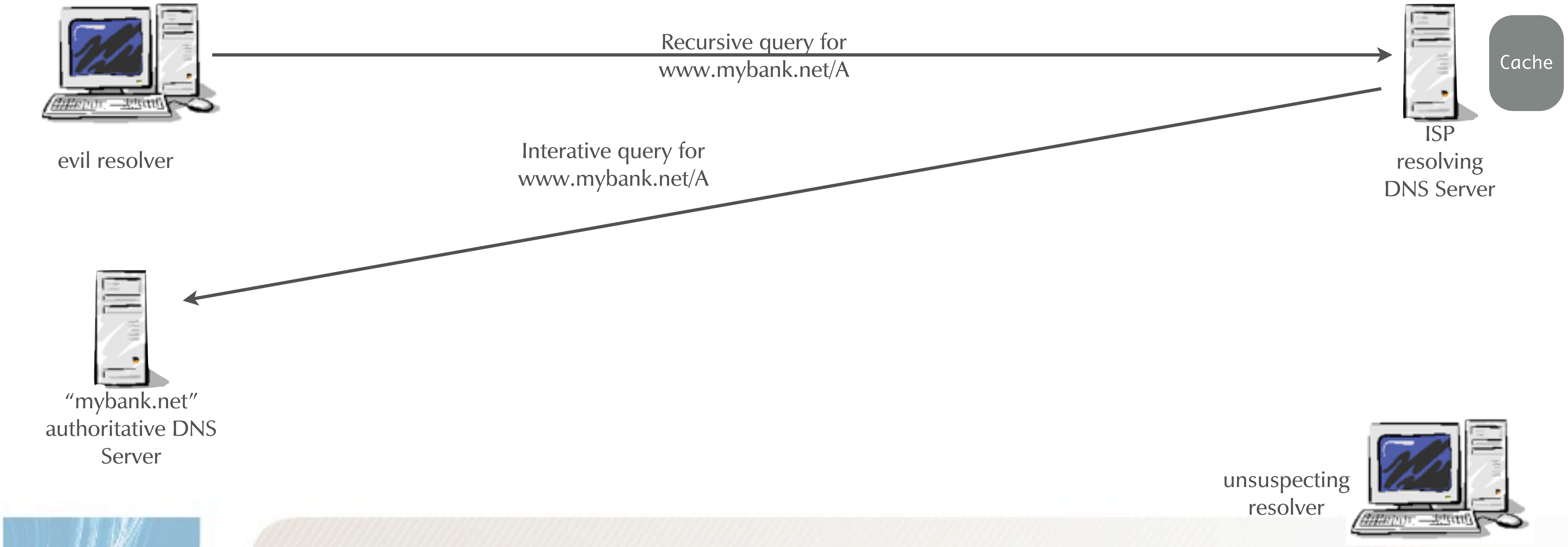
© Men & Mice http://menandmice,com

Message ID Guessing

- Any name server that receives a query from another name server knows
  - The source port it's using for queries
  - The message ID it used at some point in time
  - One query it's currently working on (Query Domainname and Query Record Type)

The Amit Klein findings (1)

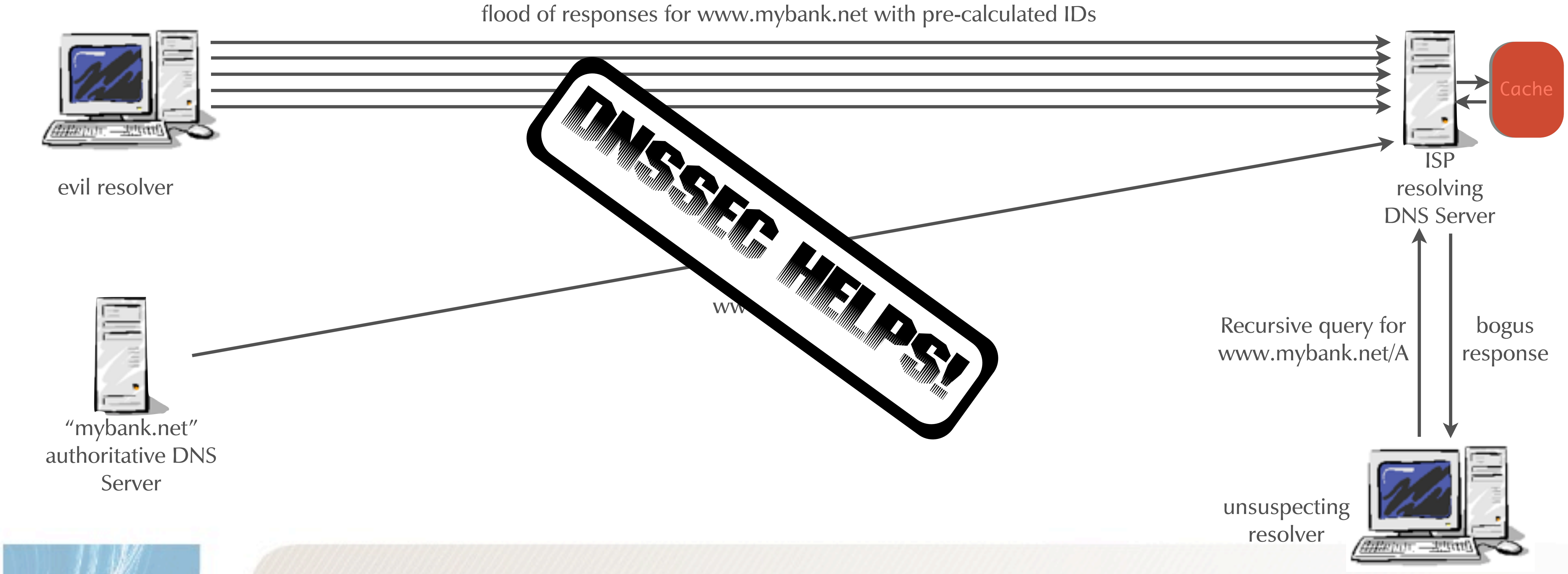
- In 2007 Amit Klein found that the randomizers used in most DNS Servers are not truly random: The next message ID's could be pre-calculated



© Men & Mice http://menandmice,com

The Amit Klein findings (2)

- In 2007 Amit Klein found that the randomizers used in most DNS Servers are not truly random: The next message ID’s could be pre-calculated



© Men & Mice http://menandmice,com

Bad randomizer

- The problem
  - The Query ID (QID) of DNS messages were not really random
    - They could be pre-calculated
- The fix
  - Better Randomizer code in the DNS Servers

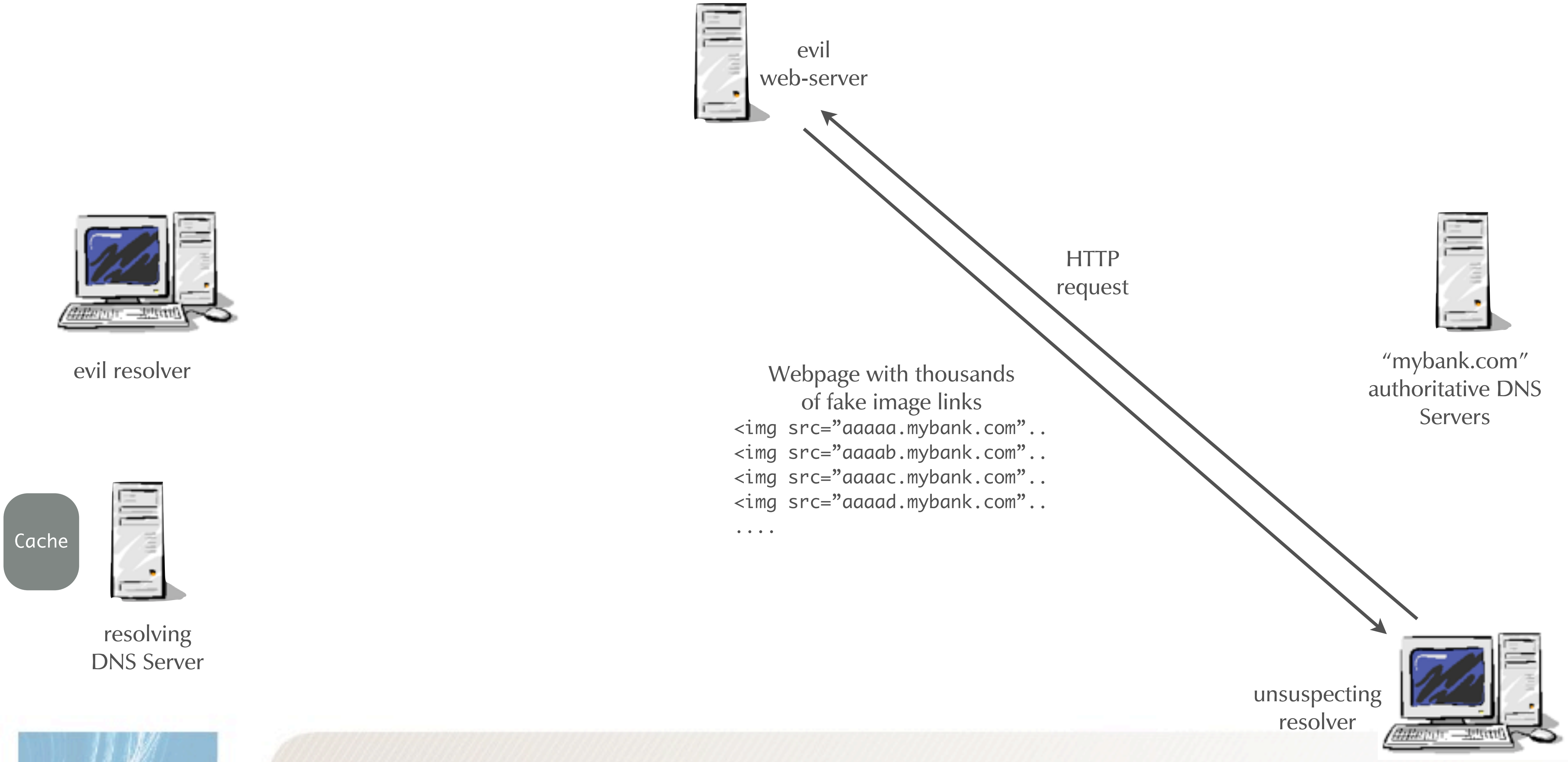
DNS Cache Spoofing
Episode III

the Dan Kaminsky findings
March-August 2008

The Dan Kaminsky findings

- Internet security researcher Dan Kaminsky found a way to spoof DNS Server caches even if the QID is truly random
  - By making the target DNS have many open outstanding queries for a domain that is 'in bailiwick' of the domain to be spoofed
- The problem
  - Even if the 16bit QID is truly random, a carefully crafted attack can fool the DNS Servers safety checks

The Dan Kaminsky findings (1)



evil
web-server

HTTP
request

evil resolver

Webpage with thousands
of fake image links

```
<img src=”aaaaa.mybank.com”..
<img src=”aaaab.mybank.com”..
<img src=”aaaac.mybank.com”..
<img src=”aaaad.mybank.com”..
....
```

“mybank.com”
authoritative DNS
Servers

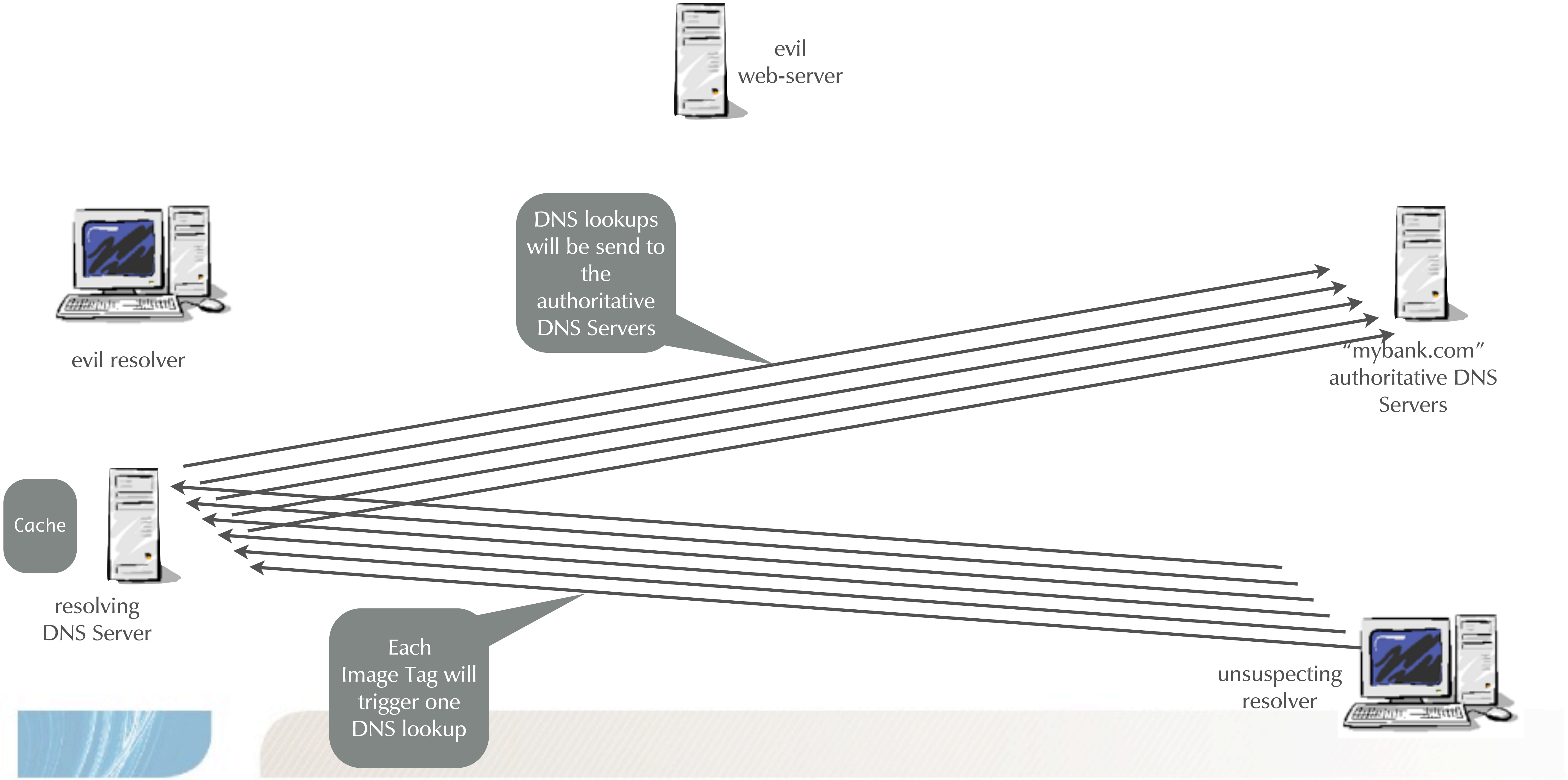
Cache

resolving
DNS Server

unsuspecting
resolver

© Men & Mice http://menandmice,com

The Dan Kaminsky findings (2)

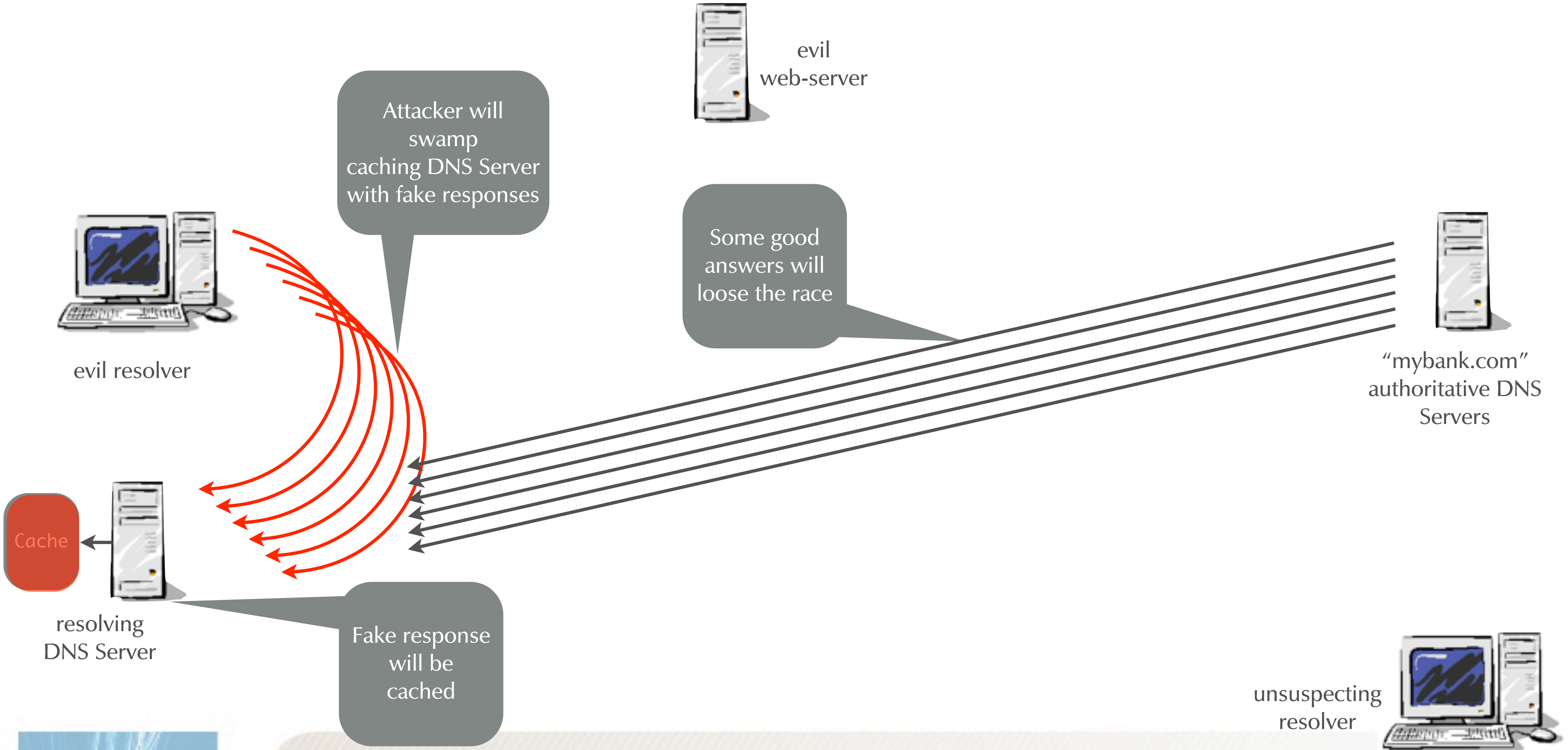


DNS lookups will be send to the authoritative DNS Servers

Each Image Tag will trigger one DNS lookup

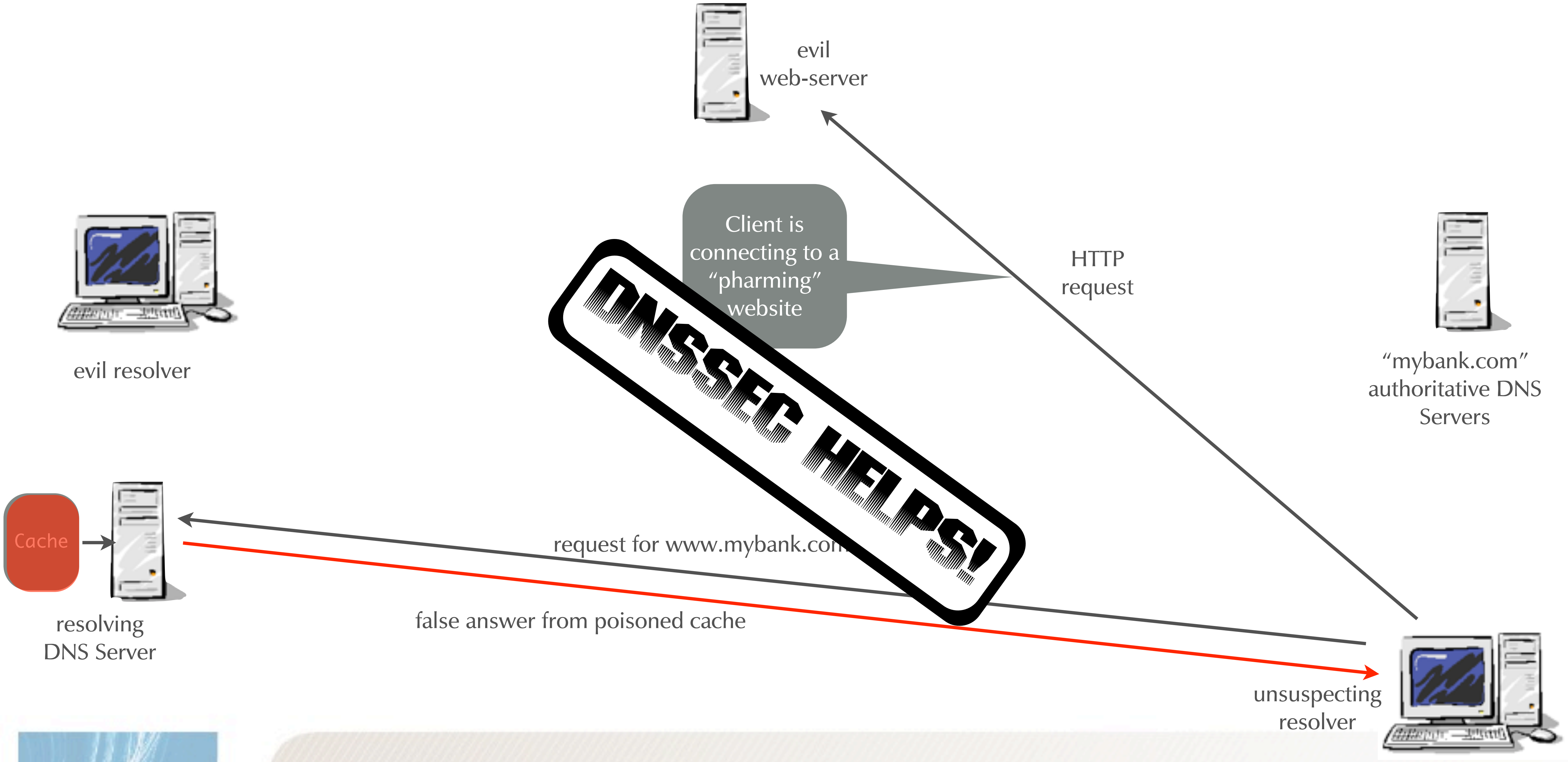
© Men & Mice http://menandmice,com

The Dan Kaminsky findings (3)



© Men & Mice http://menandmice,com

The Dan Kaminsky findings (3)


evil
web-server
Client is connecting to a "pharming" website
HTTP
request
DNSSEC HELPS!
evil resolver
"mybank.com" authoritative DNS Servers
Cache
request for www.mybank.com
resolving
DNS Server
false answer from poisoned cache
unsuspecting
resolver

© Men & Mice http://menandmice,com

the Dan Kaminsky “bug”

- Attackers try to overwrite or place a NS record in the cache

```
;; ANSWER SECTION:
aaaa.mybank.com.    120     IN    A     1.2.3.4

;; AUTHORITY SECTION:
mybank.com.         86400   IN    NS    ns1.mybank.com.
mybank.com.         86400   IN    NS    ns2.mybank.com.

;; ADDITIONAL SECTION:
ns1.mybank.com.     604800  IN    A     192.0.2.20
ns2.mybank.com.     604800  IN    A     192.0.2.30
```

high TTL for maximum damage

Here is the fake data

© Men & Mice http://menandmice,com

The Dan Kaminsky findings

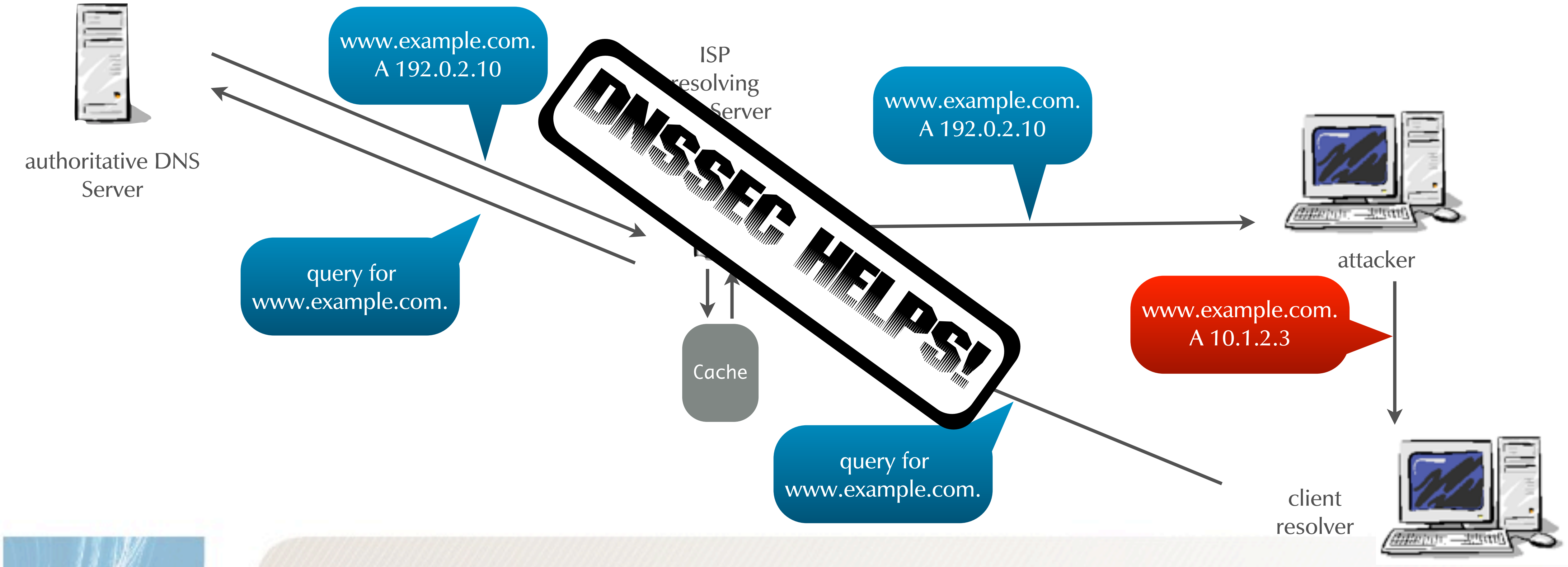
- The patch
  - Add more randomization bits
  - UDP Source Port randomization
  - Other tricks and enhancements that will add more random bits to the inter-DNS-Server communication
- The Fix
  - Deploy and use of DNSSEC (in a large scale)

“Men in the middle” attacks

- DNS Messages can be intercepted “enroute” and can be changed or altered
- “Men in the middle” attacks are easy with plain DNS
  - DNS UDP communication is “stateless”
  - Each DNS packet (query and answer) contains a full header and the query section

Men in the middle attack

- an attacker en-route can change DNS data unnoticed


authoritative DNS Server
www.example.com. A 192.0.2.10
query for www.example.com.
ISP resolving Server
DNSSEC HELPS!
Cache
www.example.com. A 192.0.2.10
attacker
www.example.com. A 10.1.2.3
query for www.example.com.
client resolver

© Men & Mice http://menandmice,com

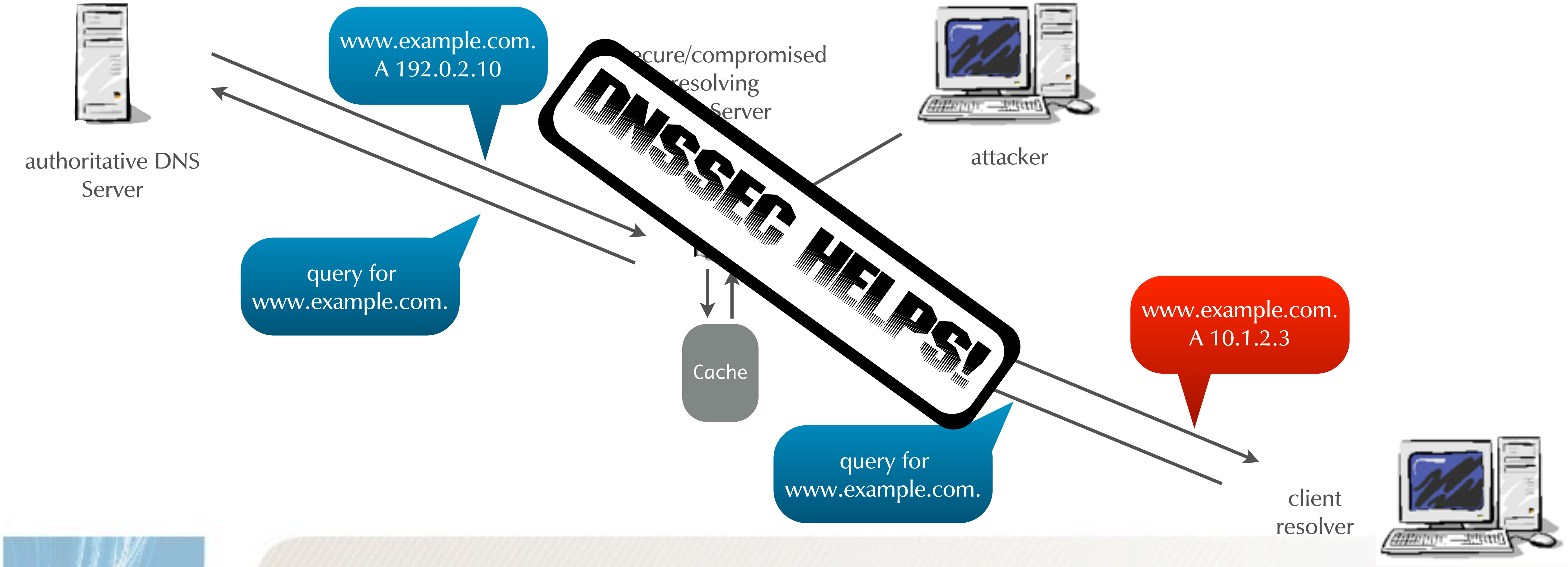
Betrayal by a trusted name server

- DNS Clients “trust” their local DNS Servers
  - But these DNS Servers can be not-so-trustworthy
    - An attacker can install a rogue DHCP Server and hand out configuration pointing to “pirate” DNS servers
    - An attacker might be able to take over an internal or external caching DNS Server, altering incoming or outgoing data, without anyone noticing (for example in a Hotel Internet Access System)
    - Viruses or Spyware can alter the local resolver configuration...
    - ... or install a small “pirate” DNS Server locally on the client

© Men & Mice http://menandmice,com

Betrayal of a trusted name server

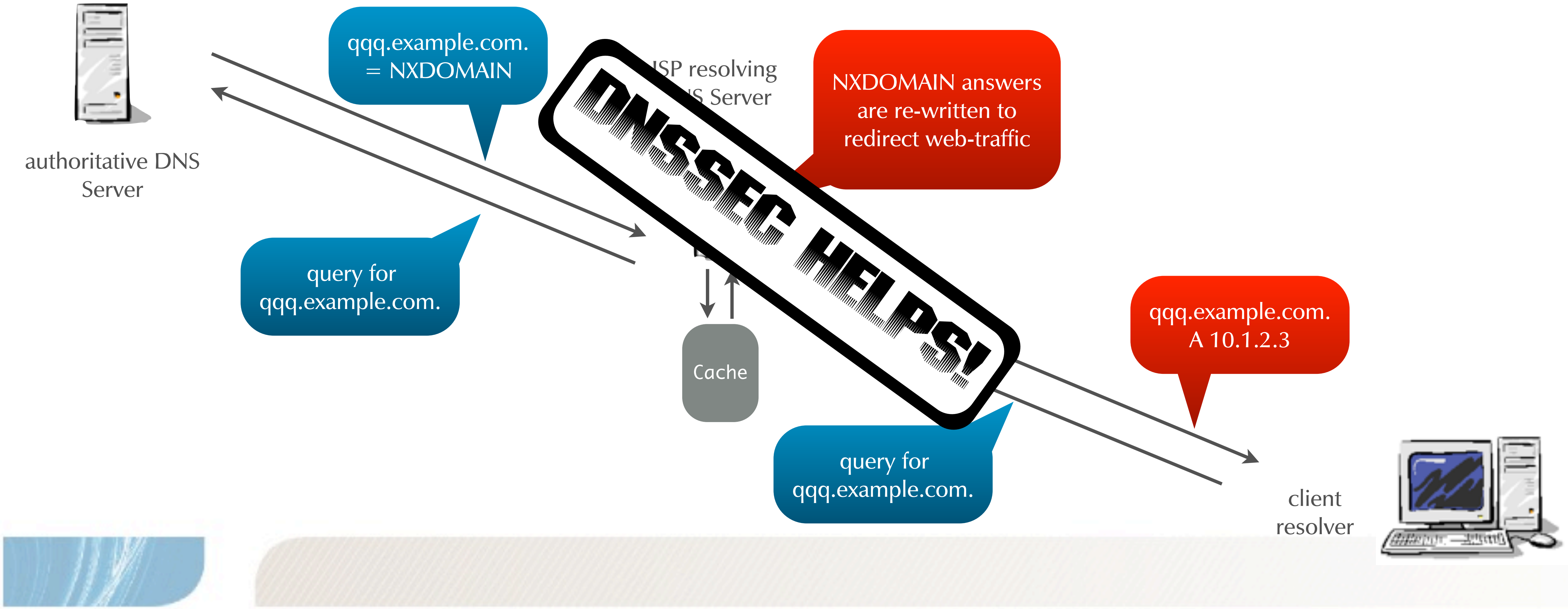
- someone in control of an resolving DNS Server has full control over the data returned


authoritative DNS Server
www.example.com. A 192.0.2.10
query for www.example.com.
ecure/compromised resolving Server
DNSSEC HELPS!
attacker
Cache
www.example.com. A 10.1.2.3
query for www.example.com.
client resolver

© Men & Mice http://menandmice,com

Betrayal of a trusted name server

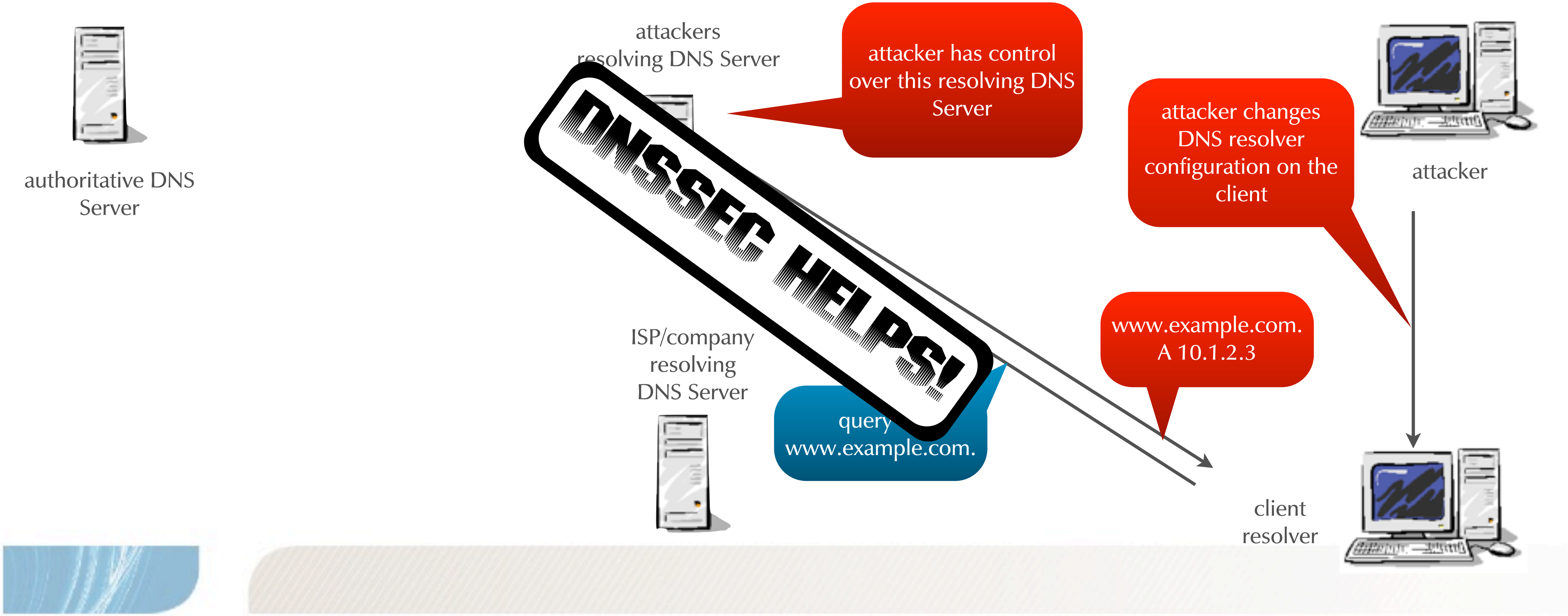
- someone in control of an resolving DNS Server has full control over the data returned


authoritative DNS Server
qqq.example.com. = NXDOMAIN
query for qqq.example.com.
ISP resolving
S Server
DNSSEC HELPS!
NXDOMAIN answers are re-written to redirect web-traffic
Cache
qqq.example.com. A 10.1.2.3
query for qqq.example.com.
client resolver

© Men & Mice http://menandmice,com

attacker changes the local resolver settings

- the local resolver settings are changed without the client user noticing, returning bad data


attackers resolving DNS Server
attacker has control over this resolving DNS Server
attacker changes DNS resolver configuration on the client
attacker
authoritative DNS Server
DNSSEC HELPS!
www.example.com. A 10.1.2.3
ISP/company resolving DNS Server
query www.example.com.
client resolver

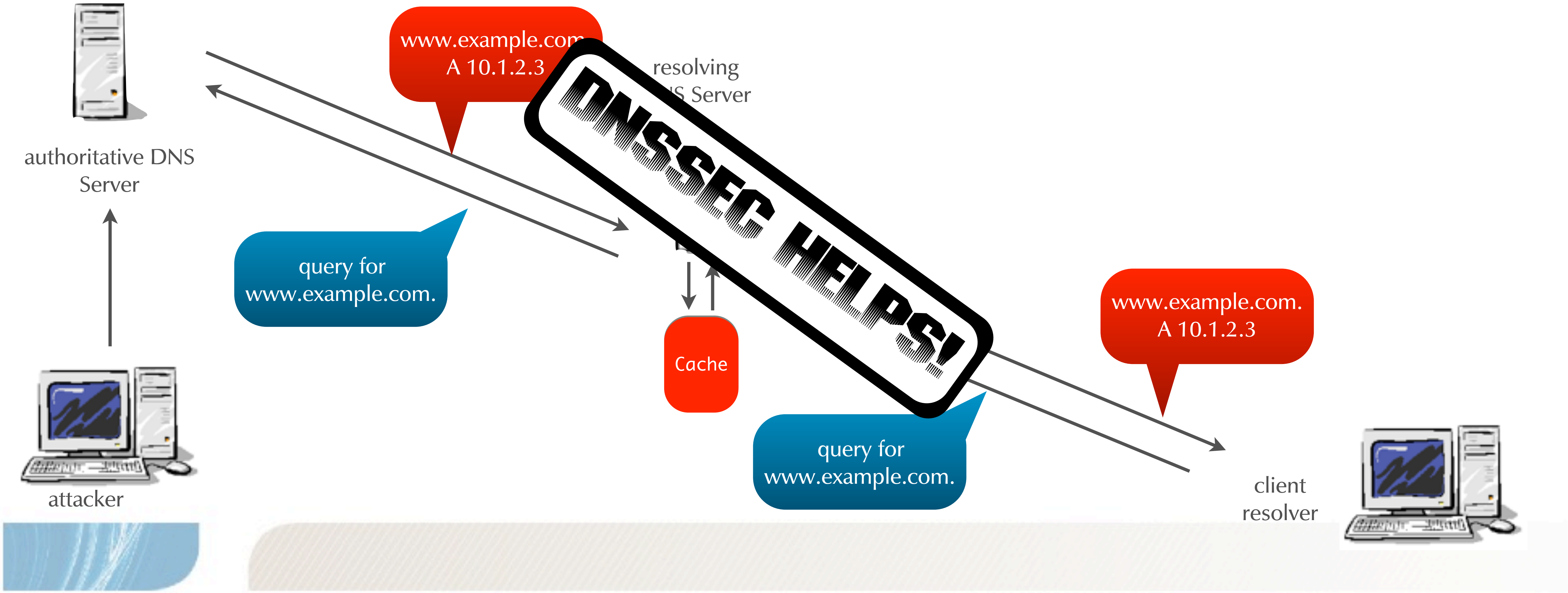
© Men & Mice http://menandmice,com

Attack on authoritative data

- attackers can us security issues to “break in” the DNS Server to alter DNS content
    - exploit security issues
        - in the operating system
        - in the DNS Server software
        - in other network software running (ssh, syslog, ...)

attack on an authoritative DNS Server

- an attacker changes the authoritative data on the DNS Server



© Men & Mice http://menandmice,com

DNSSEC

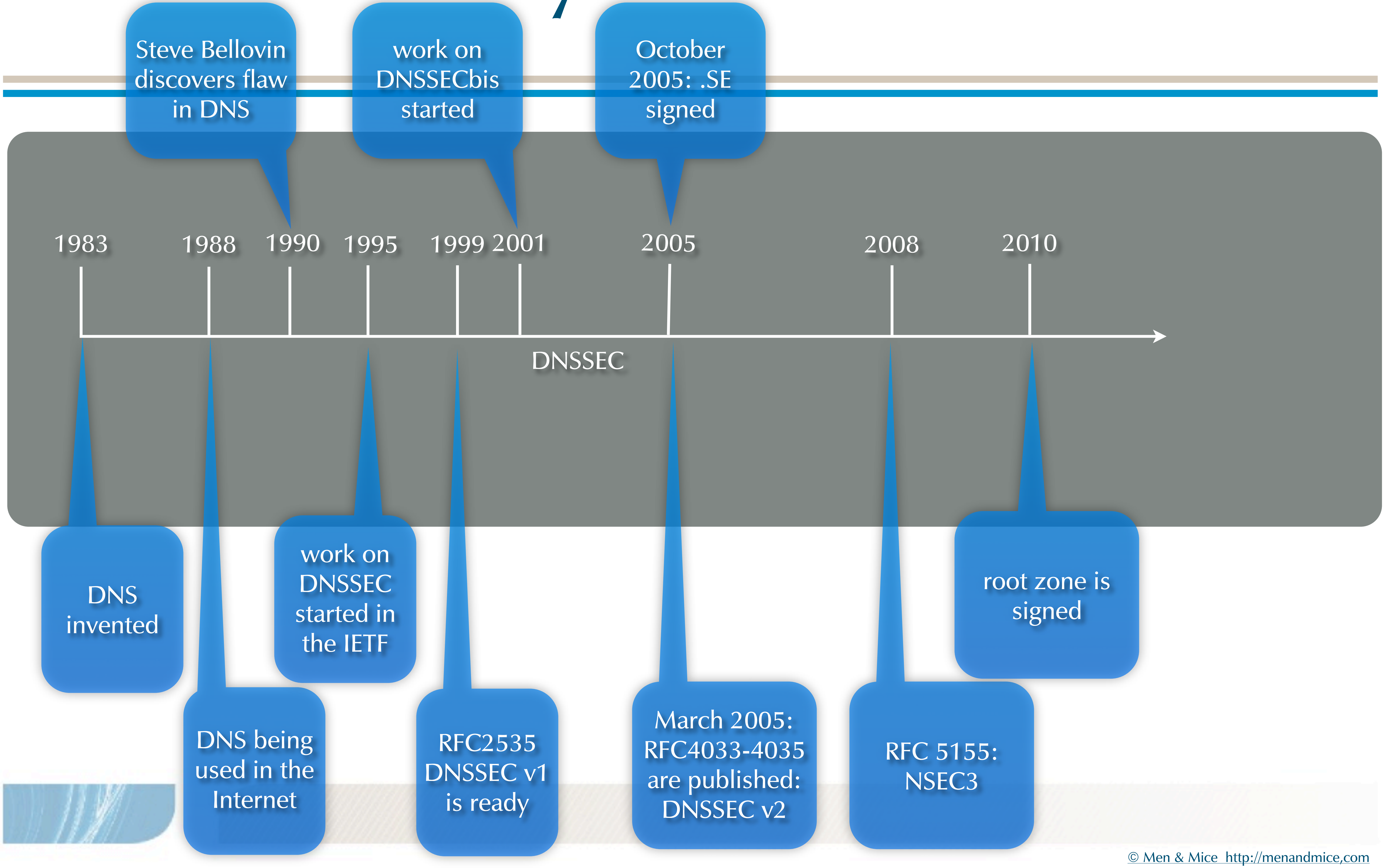
MEN&MICE

A Little Bit of History

- The original DNS protocol wasn’t designed with security in mind
- It has very few built-in security mechanisms
- As the Internet became wilder and woollier, the IETF realized this would be a problem
    - DNS spoofing was too easy, for example
- DNSSEC and later TSIG were developed to help address this problem

© Men & Mice http://menandmice,com

History of DNSSEC



DNS invented

DNS being used in the Internet

Steve Bellovin discovers flaw in DNS

work on DNSSEC started in the IETF

RFC2535 DNSSEC v1 is ready

work on DNSSECbis started

March 2005: RFC4033-4035 are published: DNSSEC v2

October 2005: .SE signed

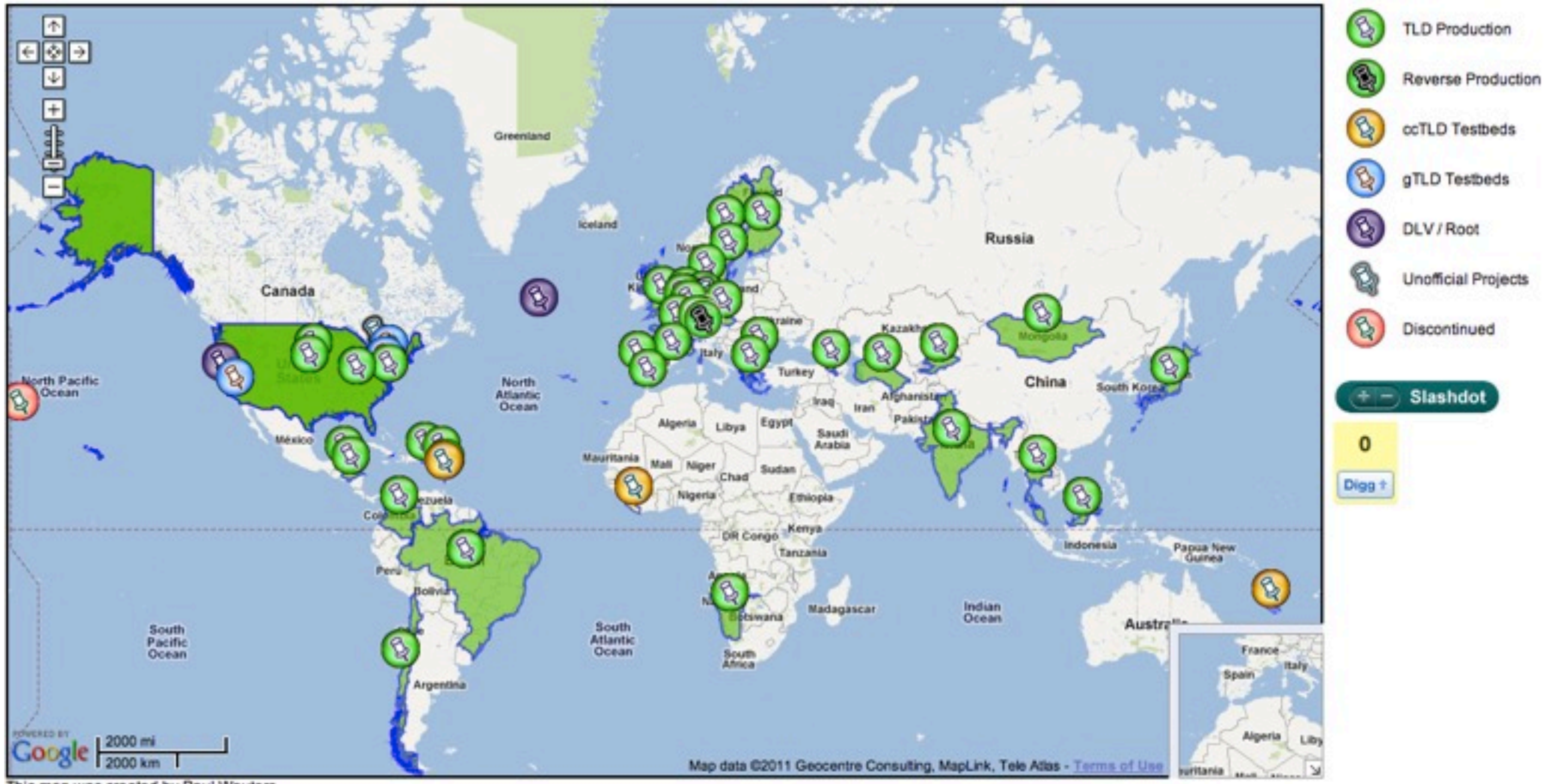
RFC 5155: NSEC3

root zone is signed

© Men & Mice http://menandmice,com

DNS Security Extensions

- DNSSEC deployment (http://www.xelerance.com/dnssec/)

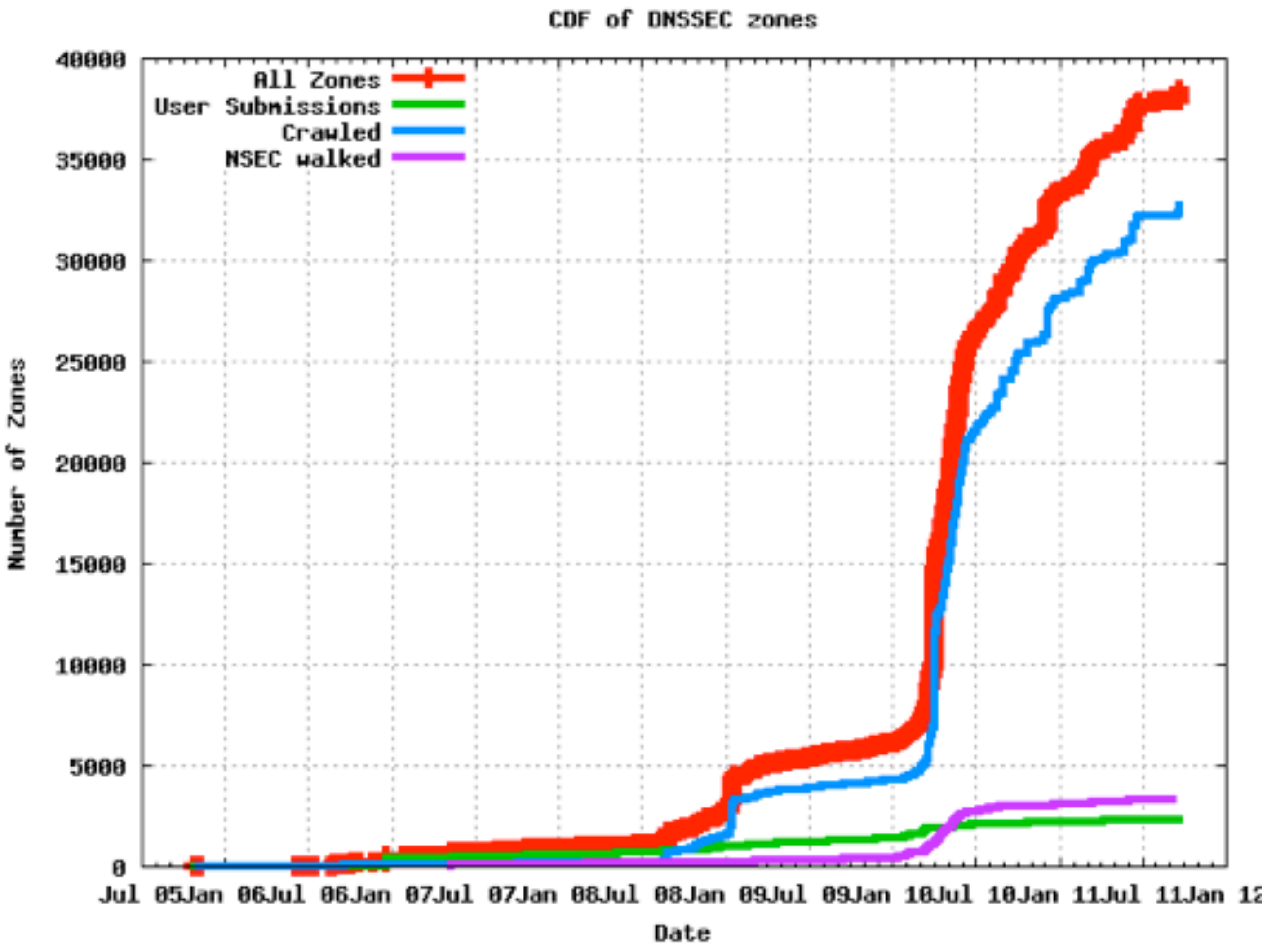


This map was created by Paul Wouters

http://en.wikipedia.org/wiki/List_of_Internet_top-level_domains

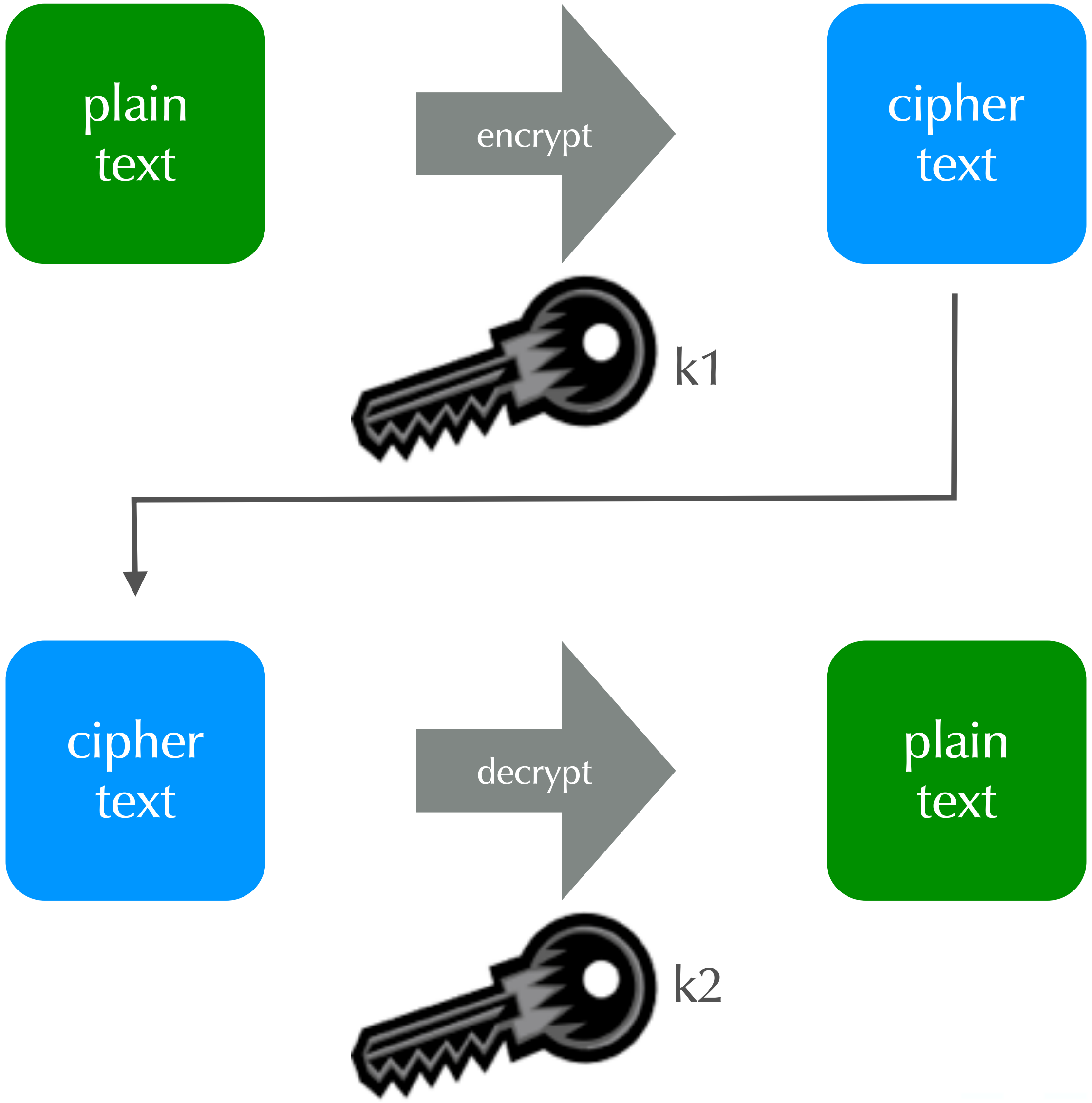
DNS Security Extensions

- DNSSEC growth http://secspider.cs.ucla.edu/images/growth.png



© Men & Mice http://menandmice,com

Public Key Cryptography Illustrated

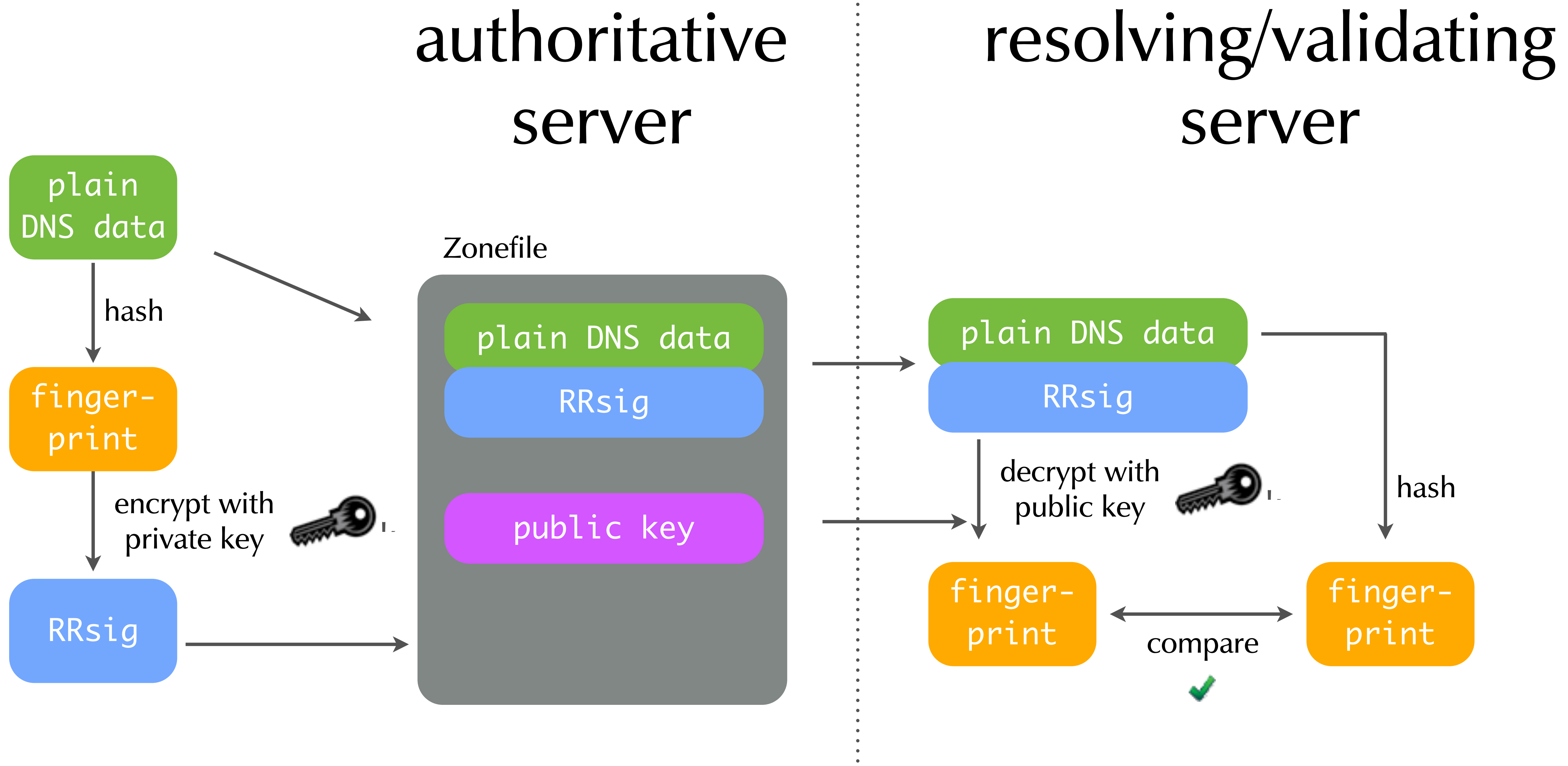


© Men & Mice http://menandmice,com

DNSSEC Validation

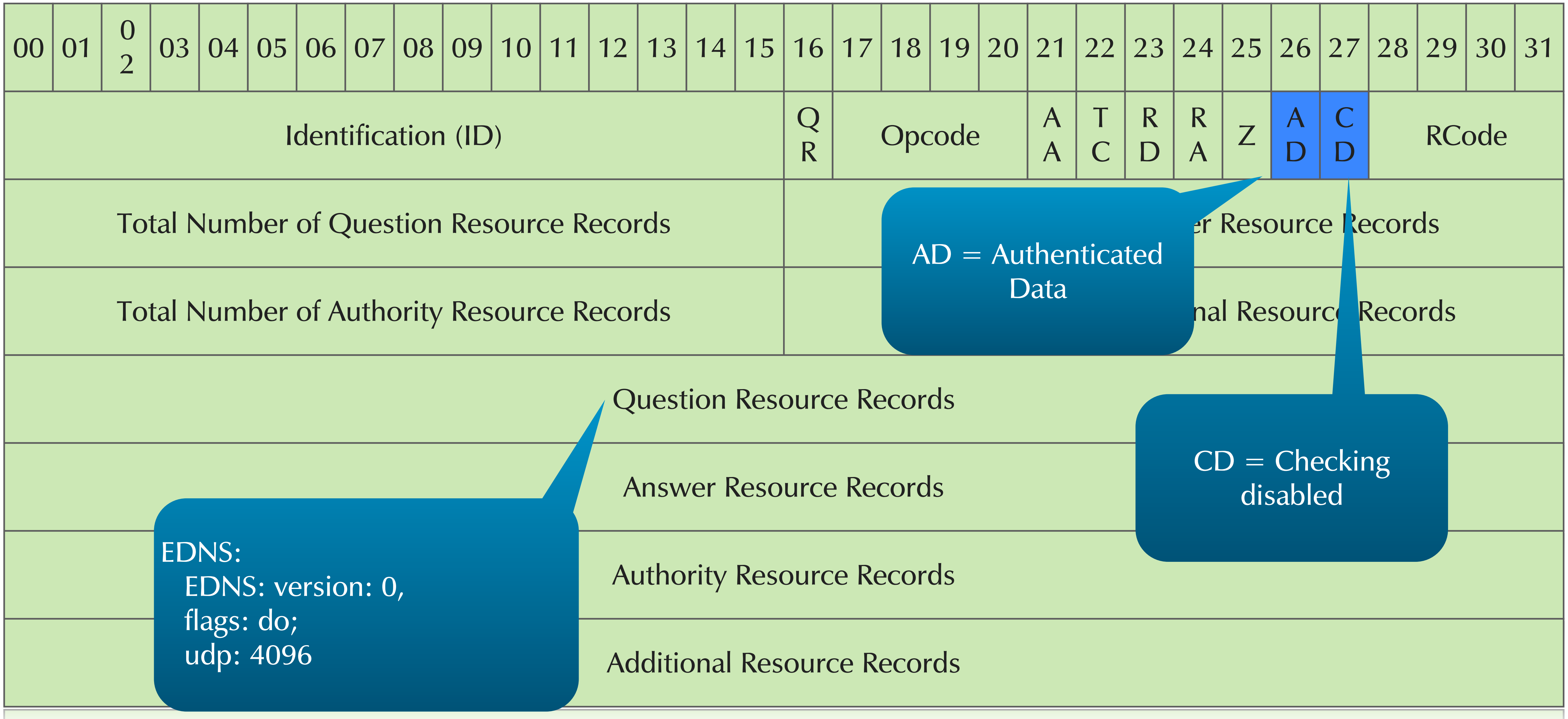
© Men & Mice http://menandmice,com

DNSSEC on one slide



© Men & Mice http://menandmice,com

DNSSEC in DNS Messages



00	01	0 2	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Identification (ID)																Q R	Opcode				A A	T C	R D	R A	Z	A D	C D	RCode			
Total Number of Question Resource Records																er Resource Records															
Total Number of Authority Resource Records																nal Resourc Records															
Question Resource Records																															
Answer Resource Records																															
Authority Resource Records																															
Additional Resource Records																															

AD = Authenticated Data

CD = Checking disabled

EDNS:
EDNS: version: 0,
flags: do;
udp: 4096

© Men & Mice http://menandmice,com

DNSSEC in DNS Messages

- DO Flag in EDNS pseudo record: **D**NSSEC **O**K
    - this client can handle DNSSEC records
    - in addition, each client signaling “DNSSEC OK” also signals that it can handle UDP DNS responses larger 512 byte

DNSSEC in DNS Messages

- AD Flag:
  - a validating resolver signaling to the client
    - that it has successfully validated the DNSSEC data
    - invalid DNSSEC data will not be send to a downstream resolver (client), instead the resolver will send a SERVFAIL error condition

DNSSEC in DNS Messages

- CD Flag:
  - an Application can signal to the resolving DNS Server that it will validate the DNSSEC information
    - the resolving DNS Server does not need to validate itself, but is free to do so

```
 dig ripe.net +dnssec
; <<>> DiG 9.7.1-P2 <<>> ripe.net +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62185
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 5, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;ripe.net.              IN    A

;; ANSWER SECTION:
ripe.net.         172800      IN    A     193.0.6.139
ripe.net.         172800      IN    RRSIG A 5 2 172800 20101108100147 20101009090147 42006 ripe.net. Jzyeu9MUjNbk[...]5eY=

;; AUTHORITY SECTION:
ripe.net.         172800      IN    NS    sns-pb.isc.org.
ripe.net.         172800      IN    NS    sunic.sunet.se.
ripe.net.         172800      IN    NS    ns-pri.ripe.net.
ripe.net.         172800      IN    NS    ns3.nic.fr.
ripe.net.         172800      IN    RRSIG NS 5 2 172800 20101108100147 20101009090147 42006 ripe.net. I7+d5+U3683o[...]r4U=

;; ADDITIONAL SECTION:
ns-pri.ripe.net.  172800      IN    A     193.0.0.195
ns-pri.ripe.net.  172800      IN    AAAA  2001:610:240:0:53::3
ns-pri.ripe.net.  172800      IN    RRSIG A 5 3 172800 20101108100147 20101009090147 42006 ripe.net. VVZ[...]jwg=
ns-pri.ripe.net.  172800      IN    RRSIG AAAA 5 3 172800 20101108100147 20101009090147 42006 ripe.net. UP/t1m[...]k3k=

;; Query time: 454 msec
;; SERVER: 192.0.2.10#53(192.0.2.10)
;; WHEN: Sat Oct  9 22:39:45 2010
;; MSG SIZE  rcvd: 870
```

AD flag: secure answer

EDNS0 information including the DO flag

MEN&MICE

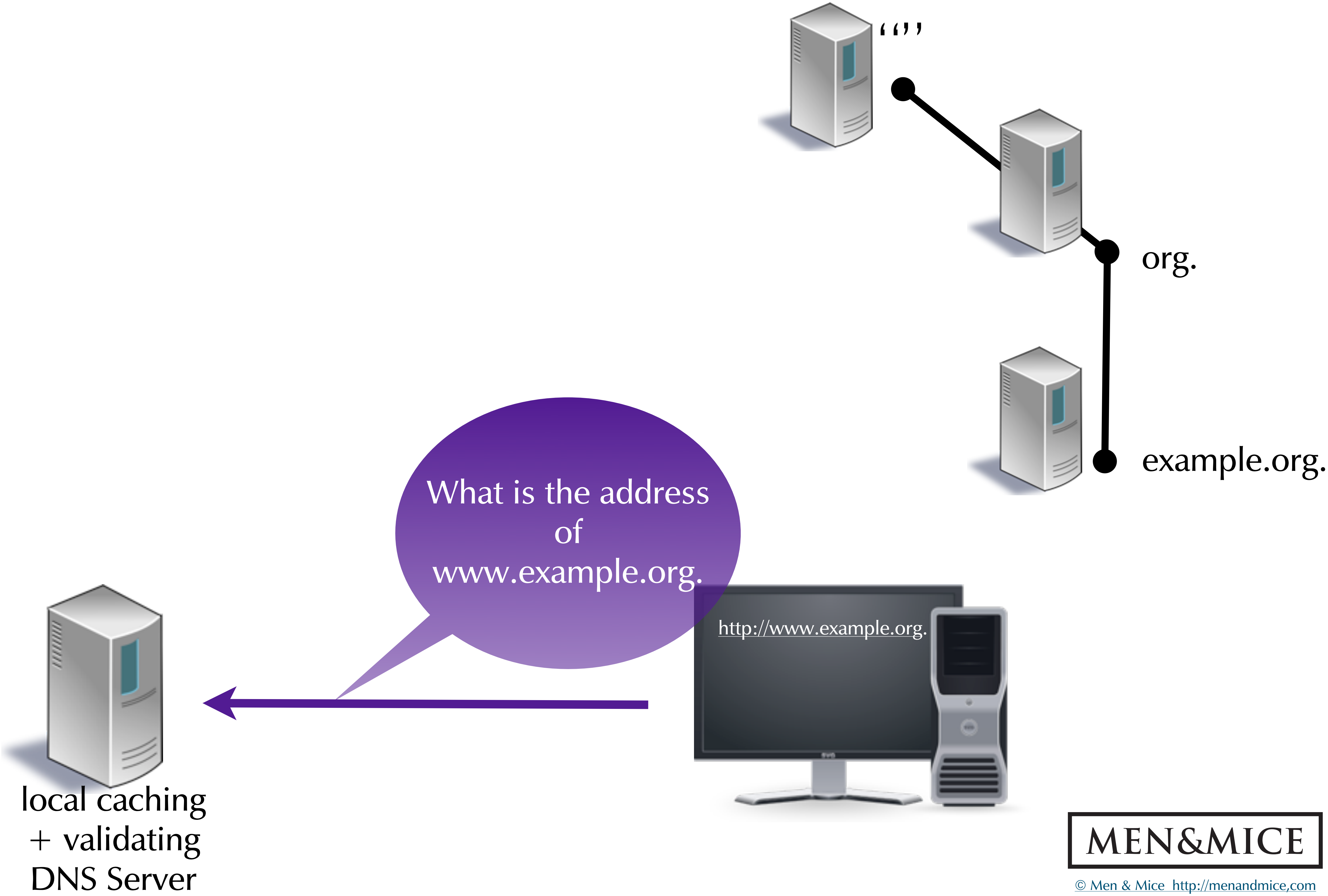
© Men & Mice http://menandmice,com

DNSSEC Name resolution (simplified)

MEN&MICE

© Men & Mice http://menandmice,com

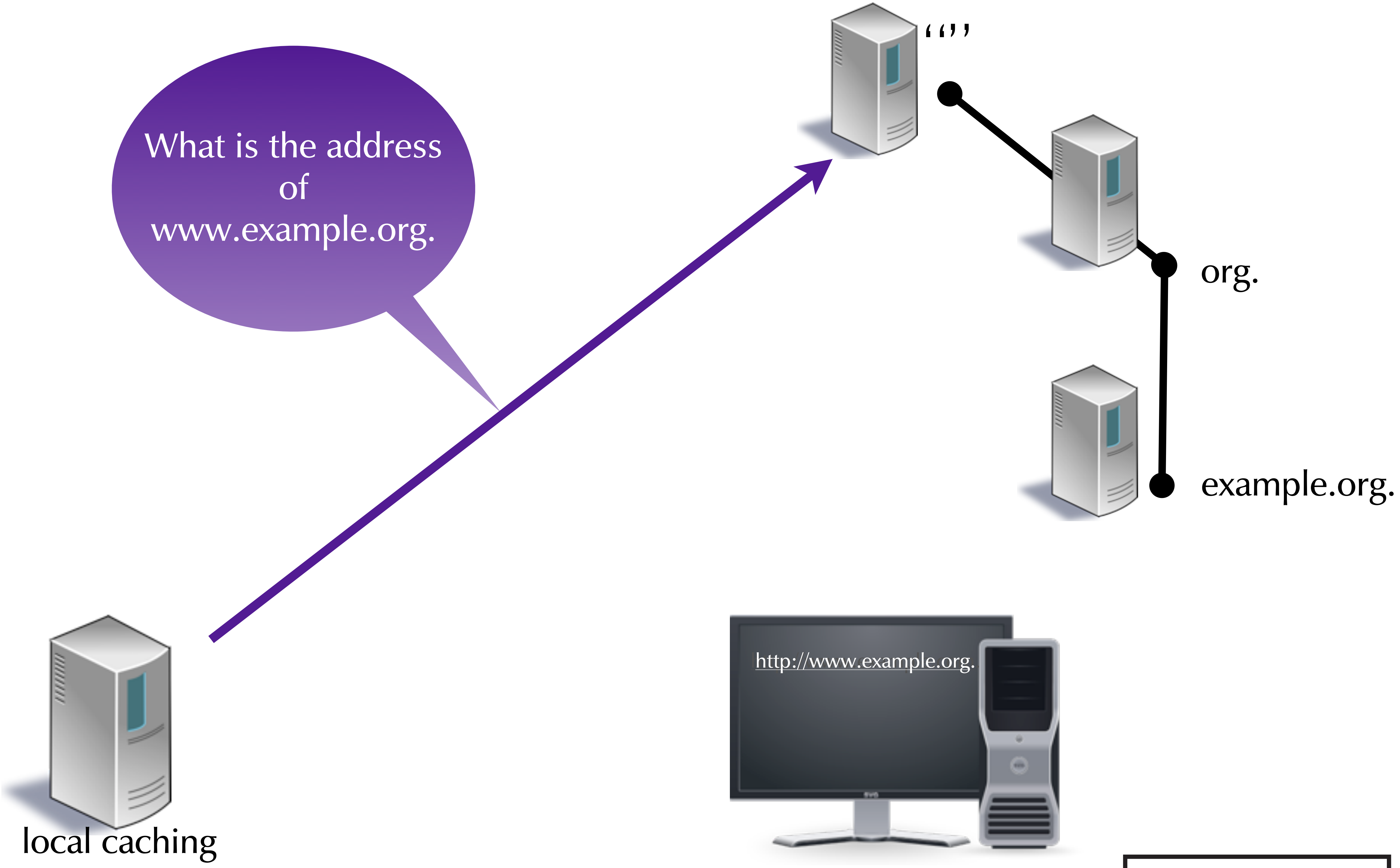
DNSSEC Name Resolution


"."
org.
example.org.
What is the address of www.example.org.
http://www.example.org.
local caching + validating DNS Server

MEN&MICE

© Men & Mice http://menandmice,com

DNSSEC Name Resolution



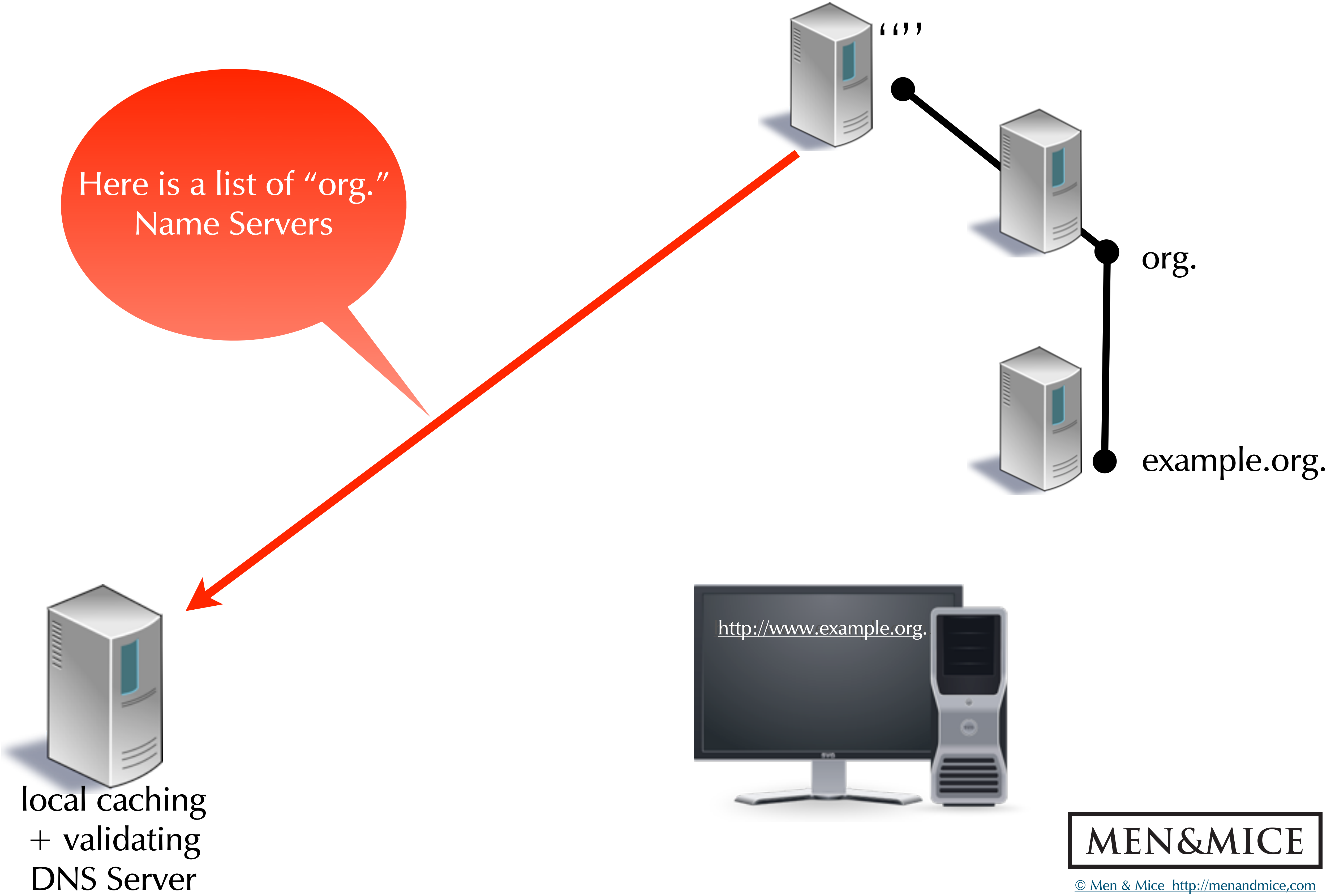
What is the address of www.example.org.

local caching + validating DNS Server

MEN&MICE

© Men & Mice http://menandmice,com

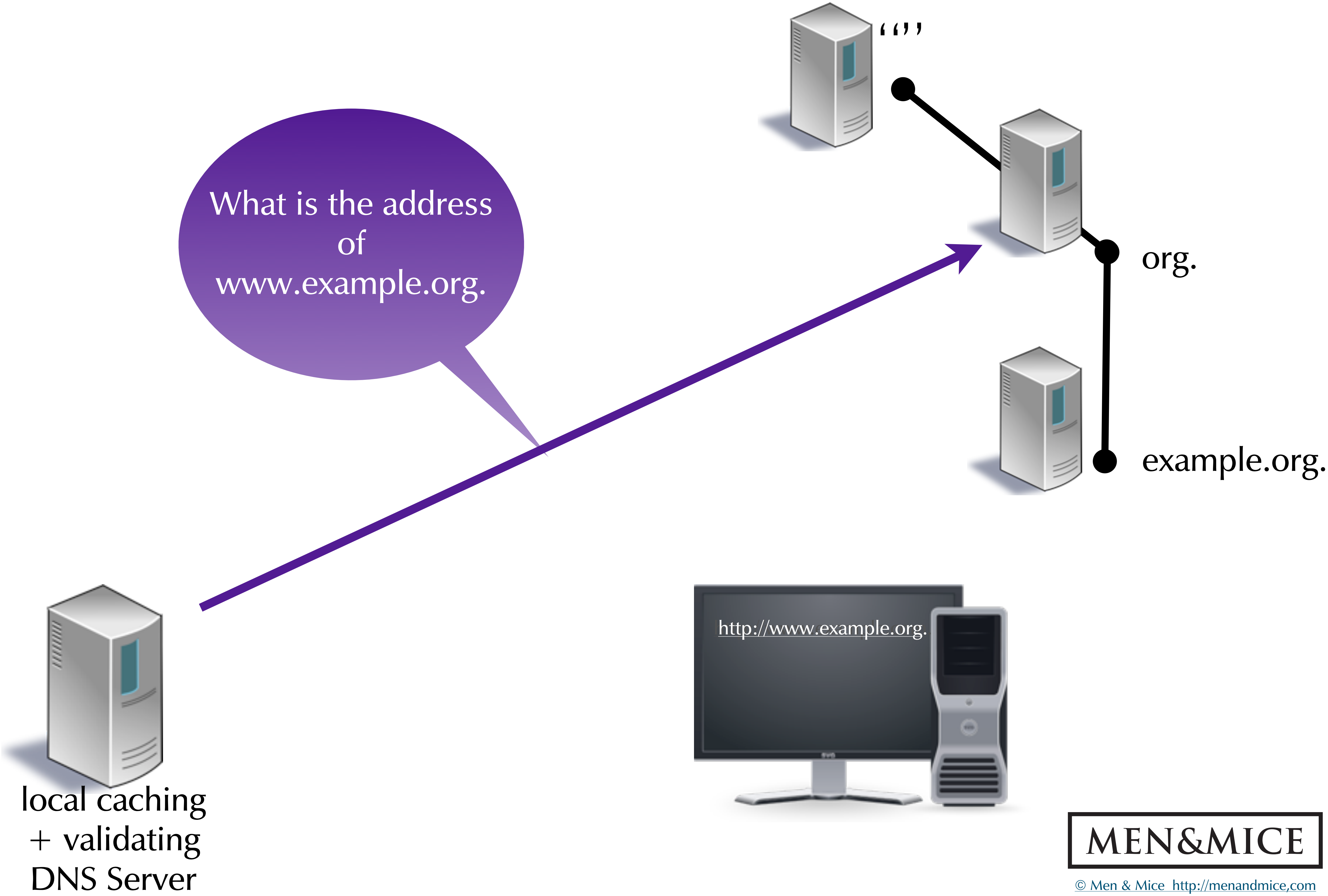
DNSSEC Name Resolution


“.”
Here is a list of “org.” Name Servers
org.
example.org.
http://www.example.org.
local caching + validating DNS Server

MEN&MICE

© Men & Mice http://menandmice,com

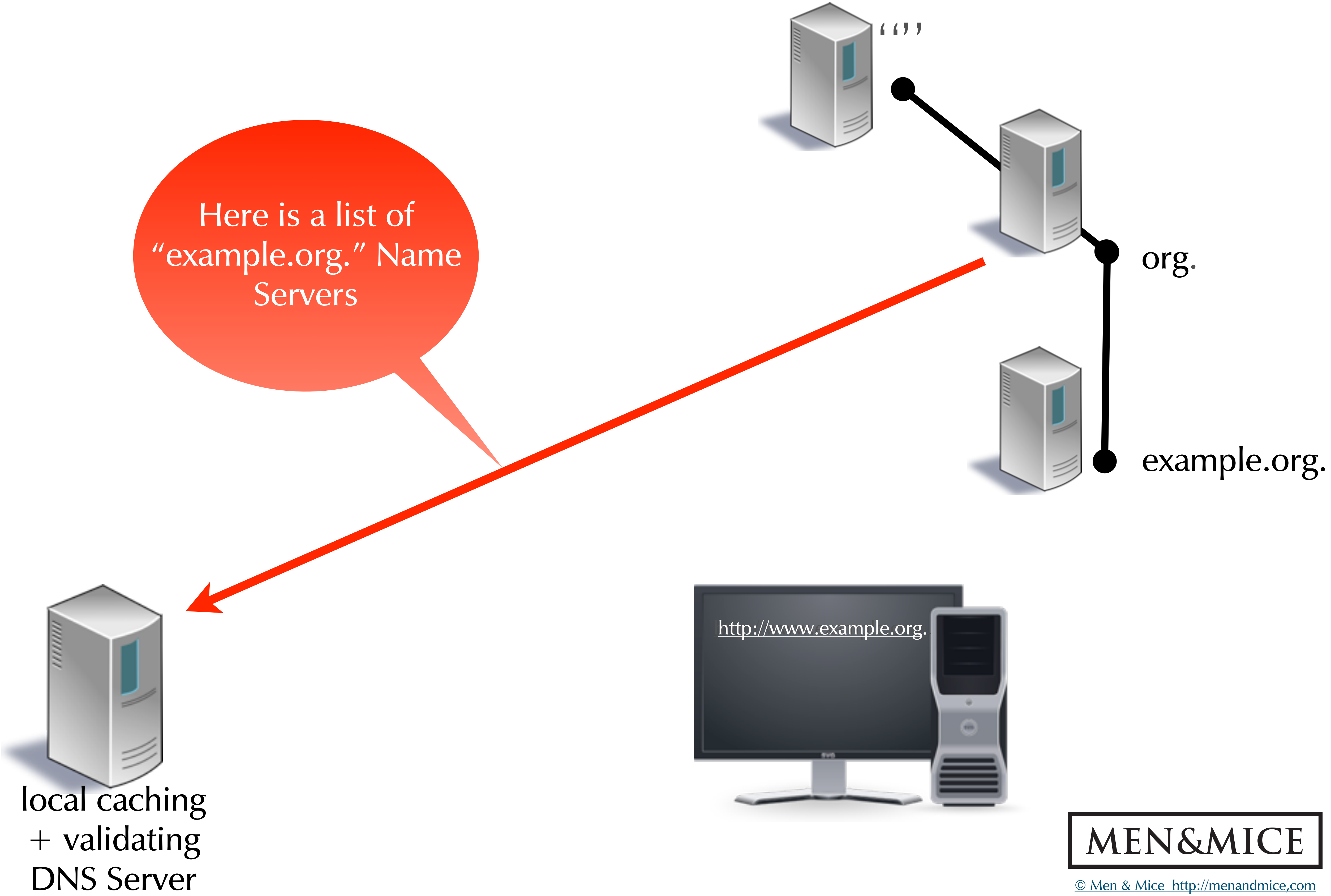
DNSSEC Name Resolution


"."
org.
example.org.
What is the address of www.example.org.
http://www.example.org.
local caching + validating DNS Server

MEN&MICE

© Men & Mice http://menandmice,com

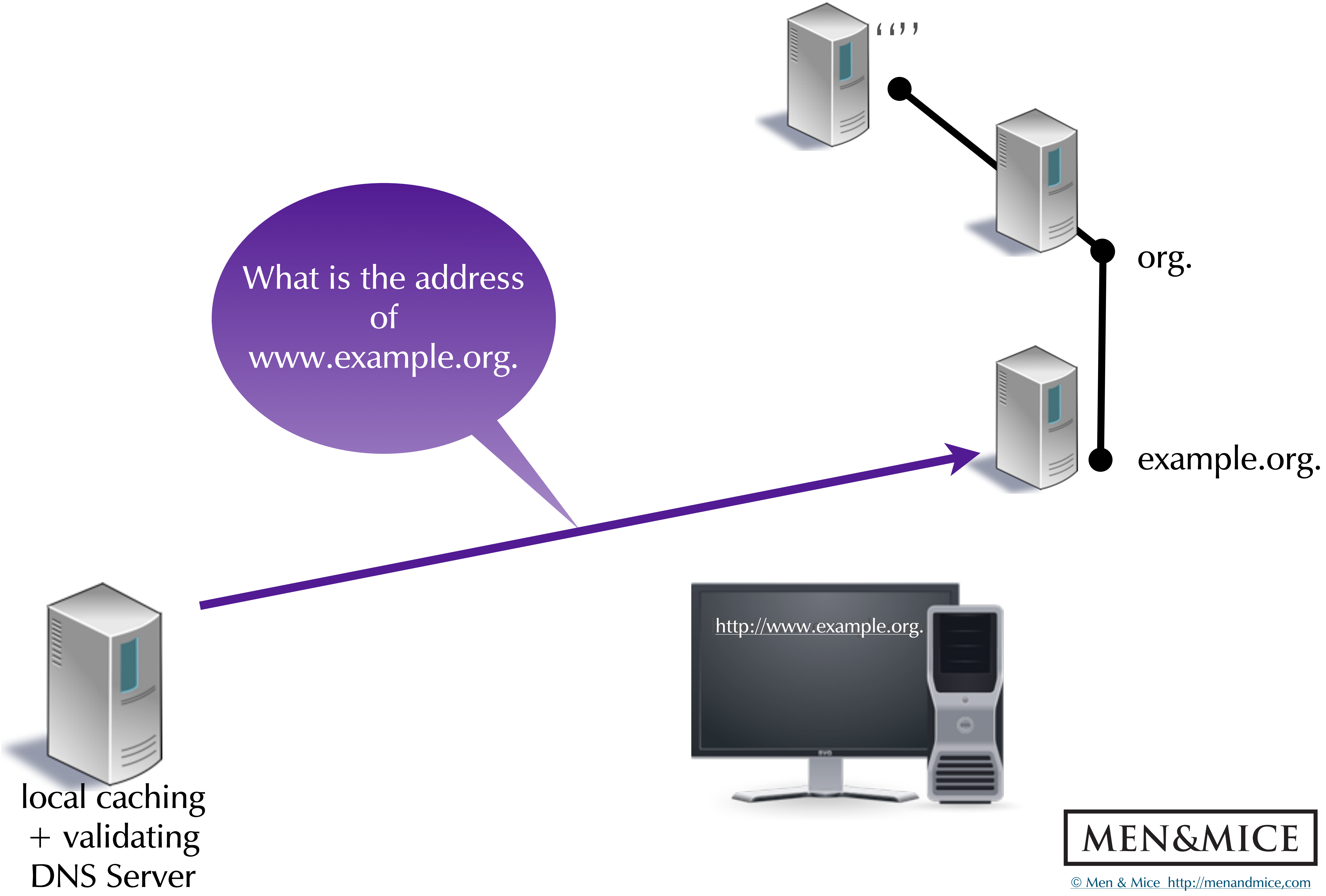
DNSSEC Name Resolution


"."
org.
example.org.
Here is a list of "example.org." Name Servers
http://www.example.org.
local caching + validating DNS Server

MEN&MICE

© Men & Mice http://menandmice,com

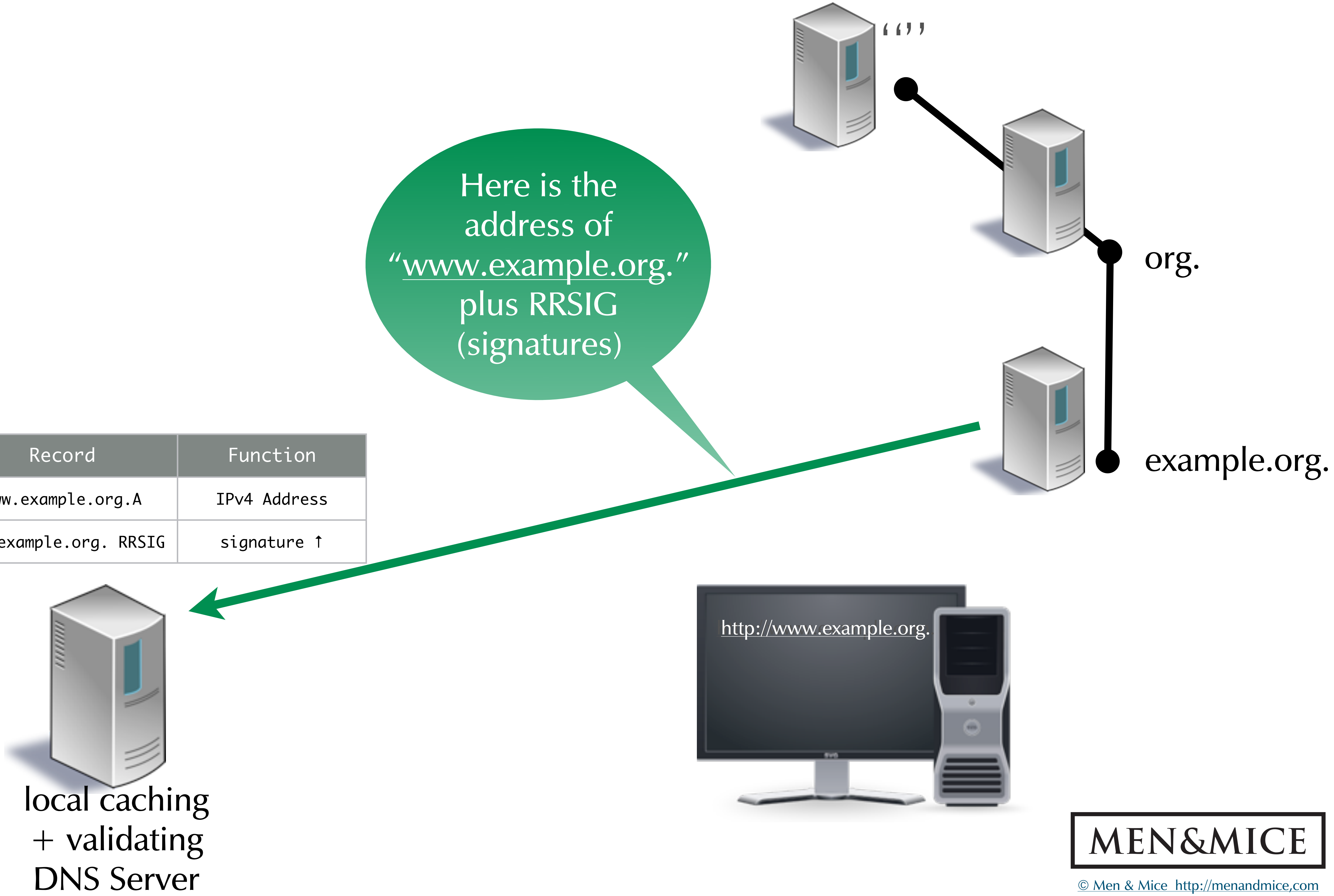
DNSSEC Name Resolution


"."
org.
example.org.
What is the address of www.example.org.
http://www.example.org.
local caching + validating DNS Server

MEN&MICE

© Men & Mice http://menandmice,com

DNSSEC Name Resolution



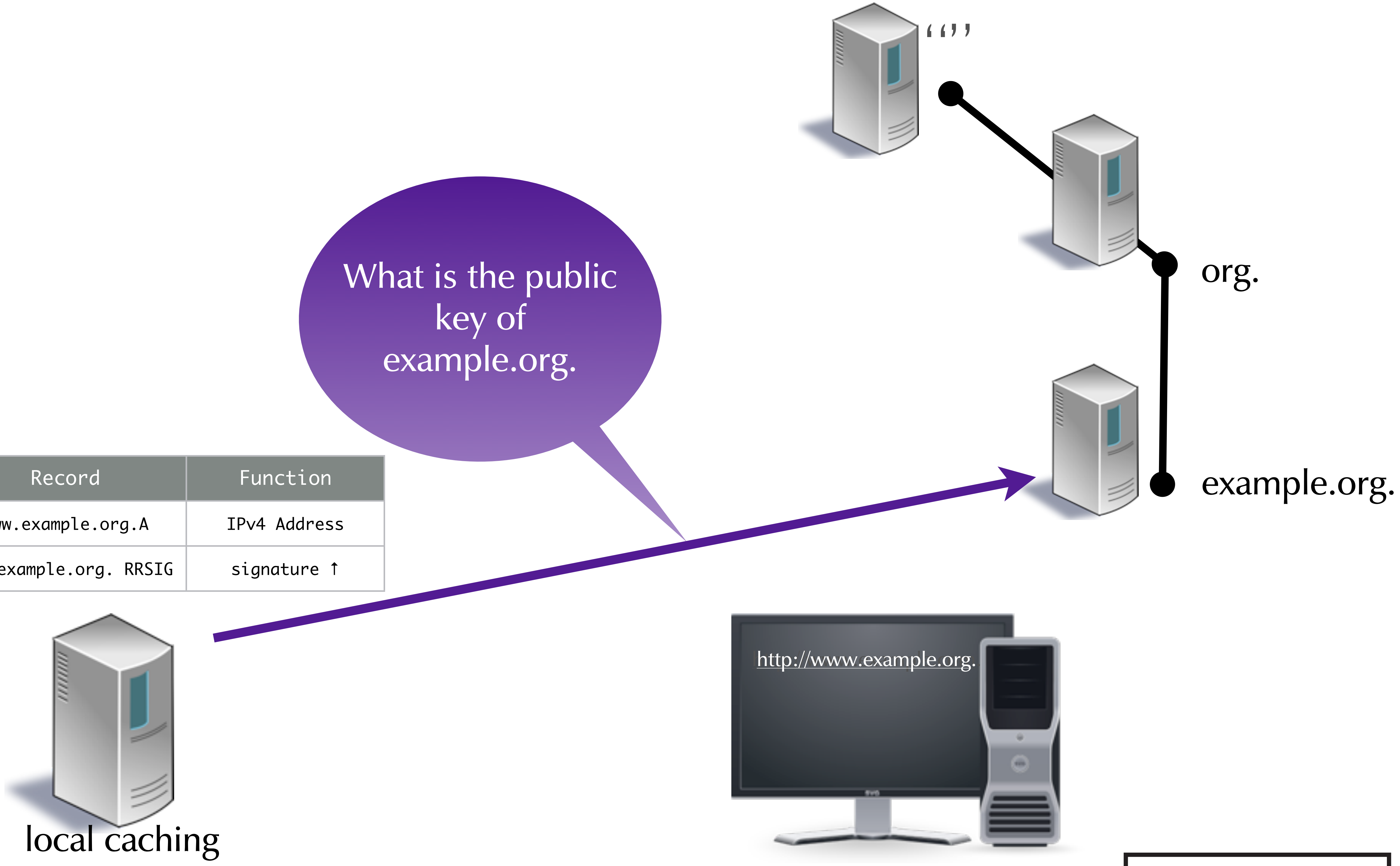
Here is the address of "www.example.org." plus RRSIG (signatures)

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑

MEN&MICE

© Men & Mice http://menandmice,com

DNSSEC Name Resolution



What is the public key of example.org.

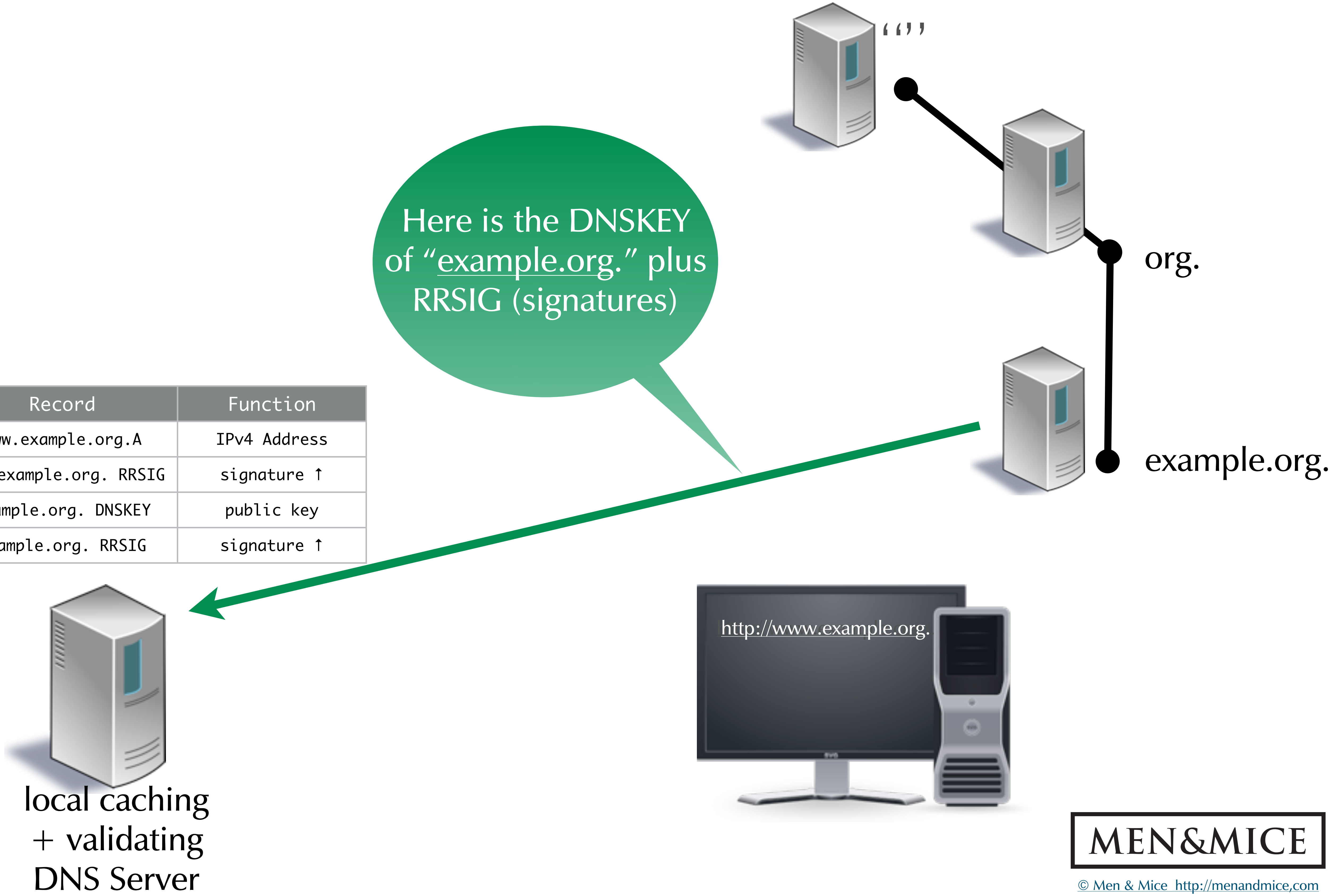
Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑

local caching
+ validating
DNS Server

MEN&MICE

© Men & Mice http://menandmice,com

DNSSEC Name Resolution



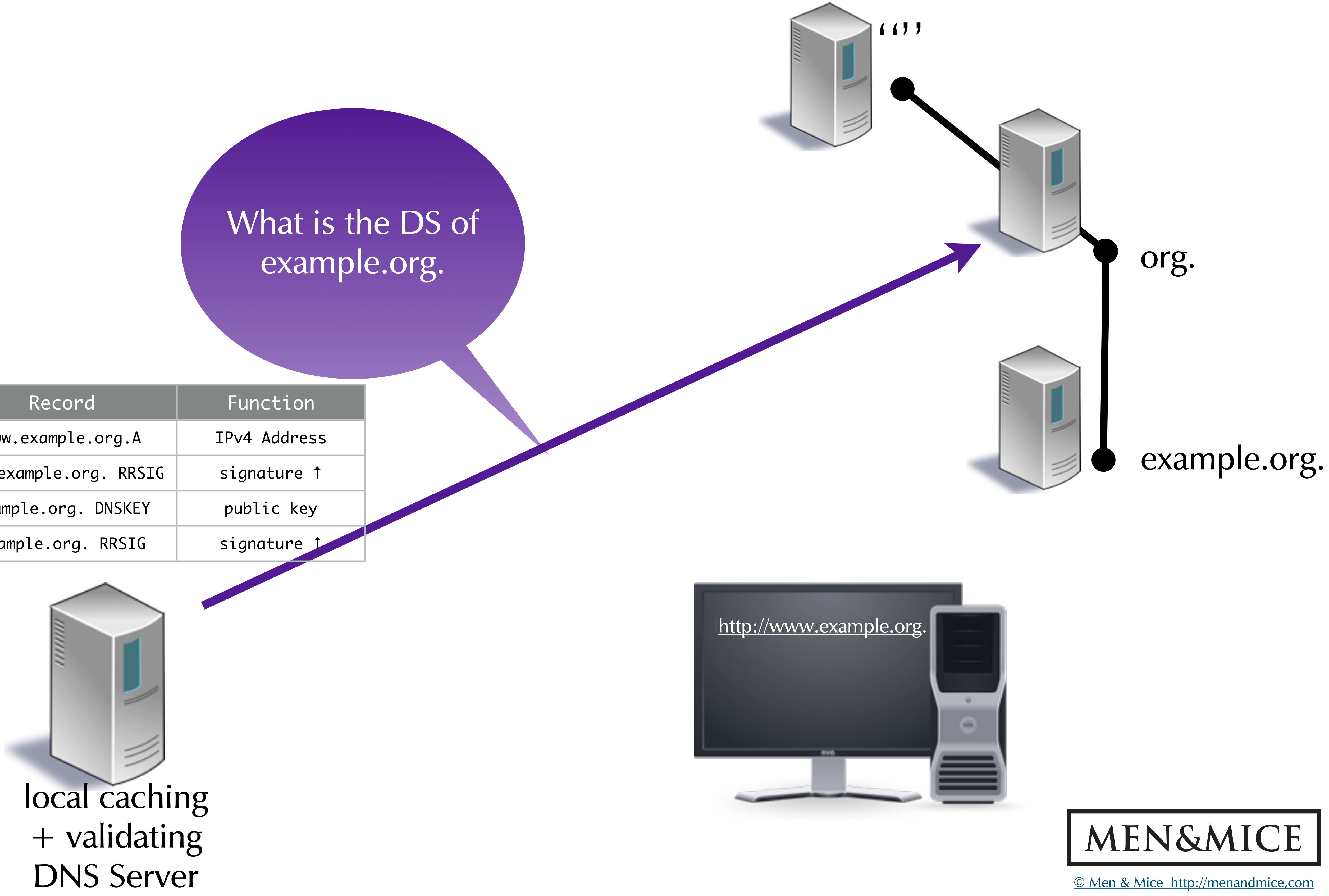
Here is the DNSKEY of "example.org." plus RRSIG (signatures)

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑

MEN&MICE

© Men & Mice http://menandmice,com

DNSSEC Name Resolution

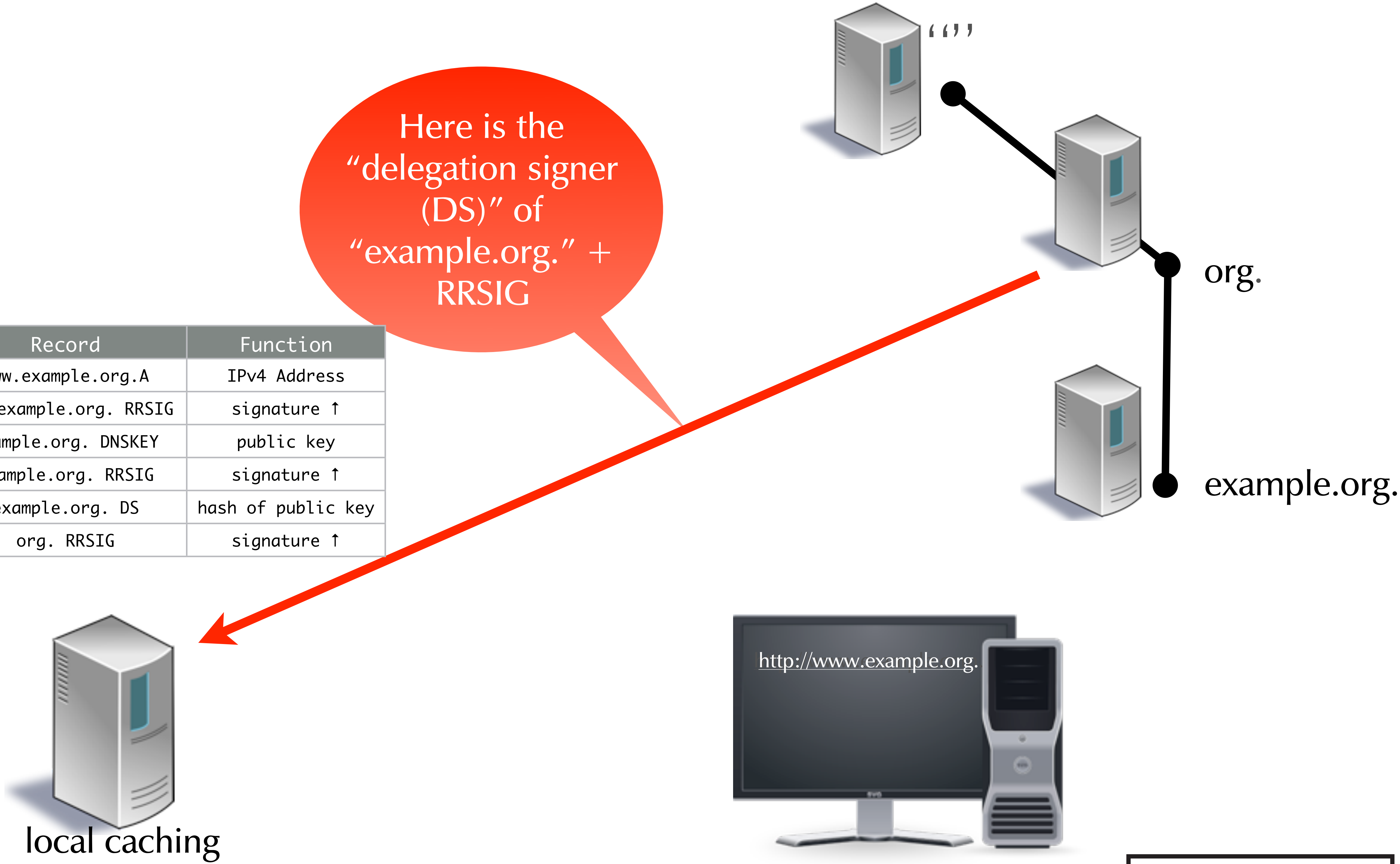


Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑

MEN&MICE

© Men & Mice http://menandmice,com

DNSSEC Name Resolution

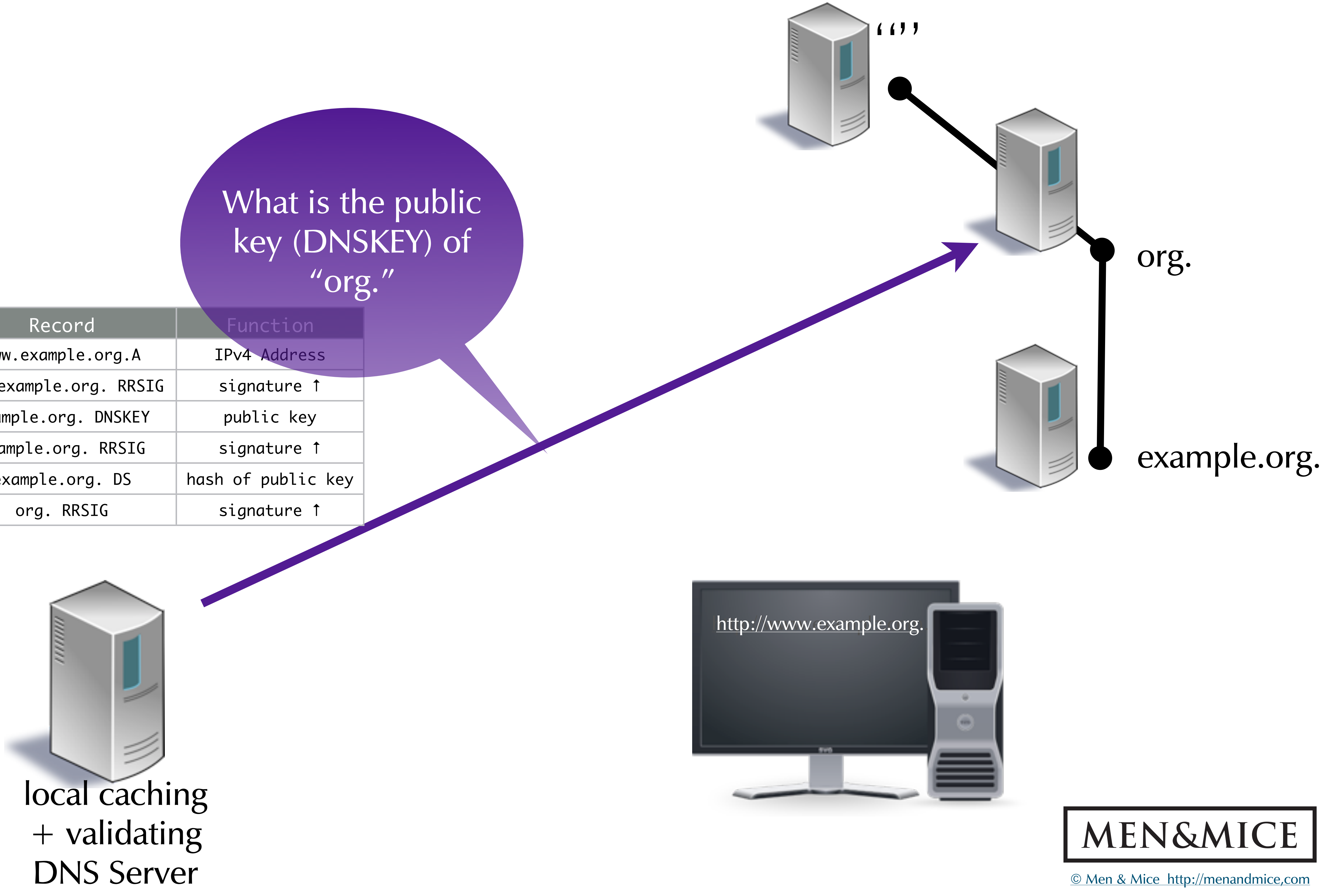


Here is the “delegation signer (DS)” of “example.org.” + RRSIG

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑

MEN&MICE
© Men & Mice http://menandmice,com

DNSSEC Name Resolution



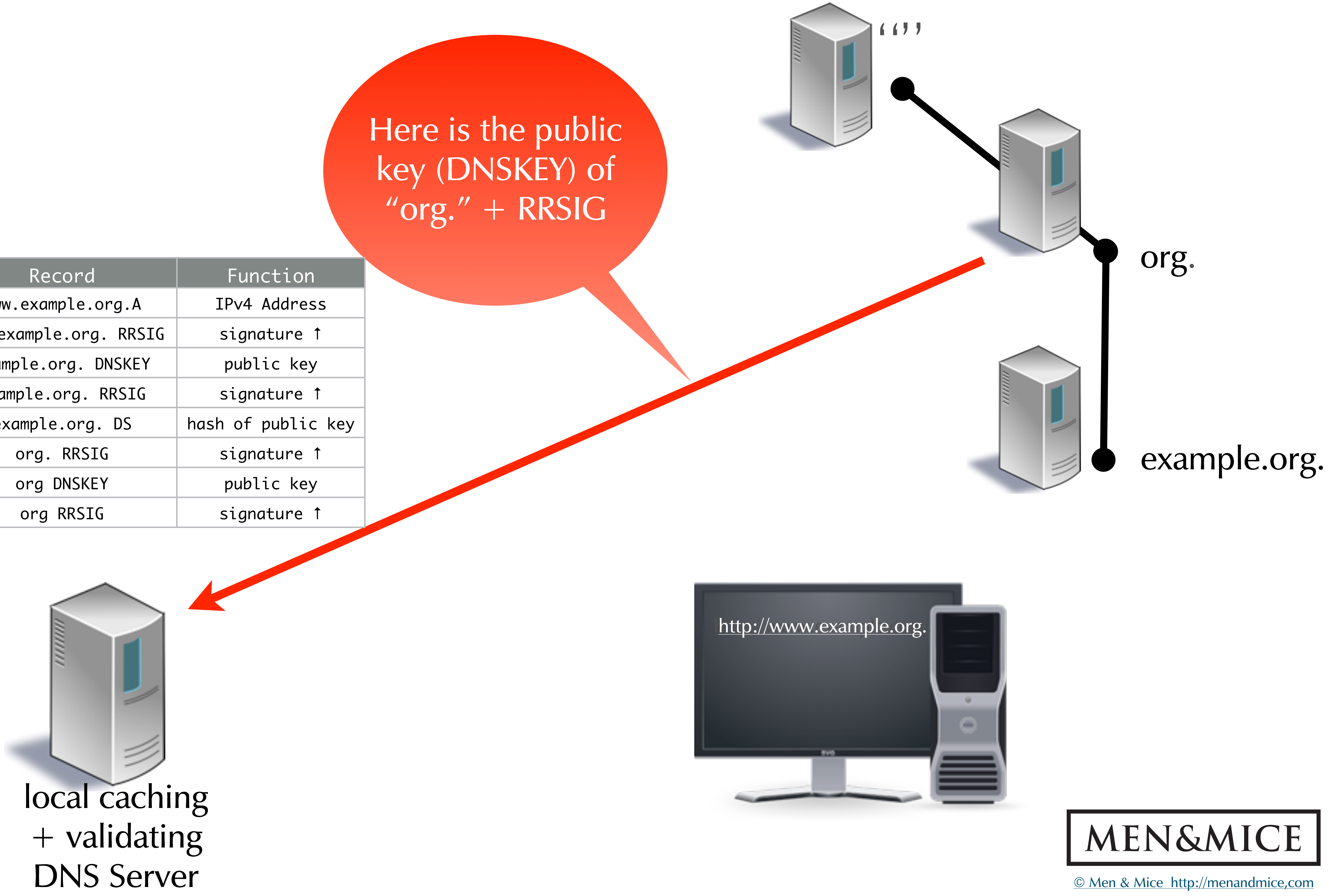
What is the public key (DNSKEY) of “org.”

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑

MEN&MICE
© Men & Mice http://menandmice,com

DNSSEC Name Resolution

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑



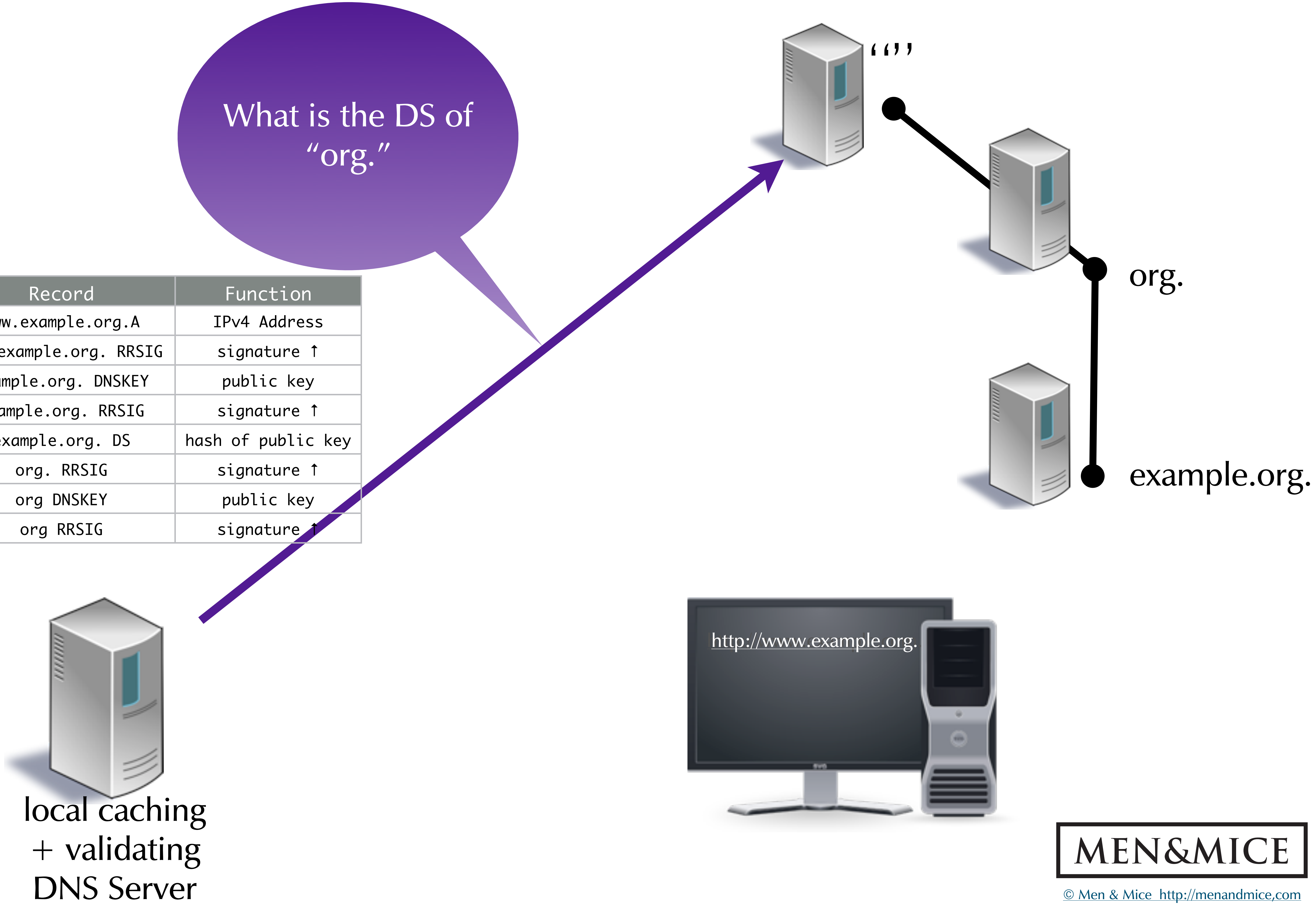
Here is the public key (DNSKEY) of “org.” + RRSIG

local caching
+ validating
DNS Server

MEN&MICE

© Men & Mice http://menandmice,com

DNSSEC Name Resolution



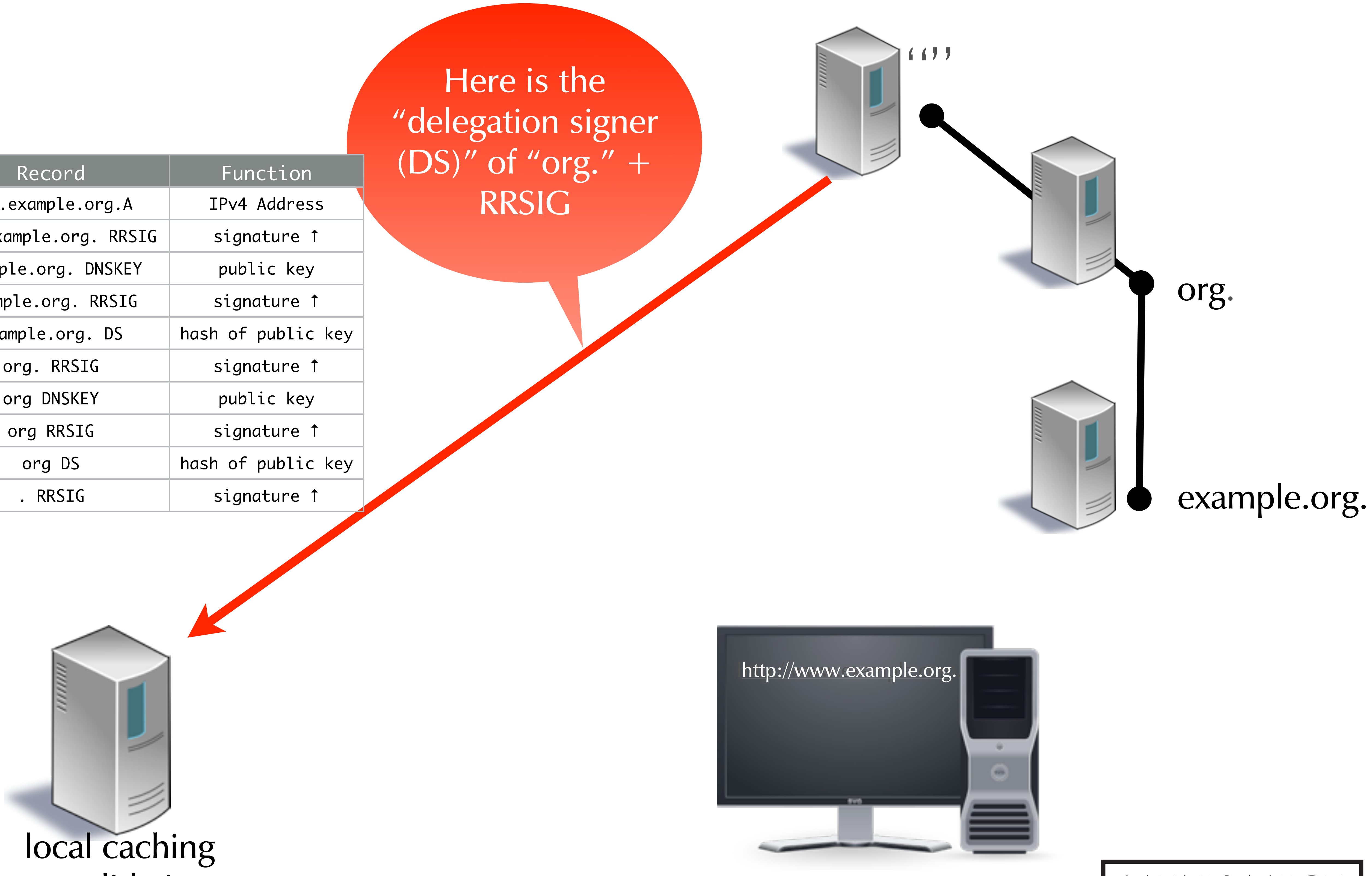
Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑

MEN&MICE

© Men & Mice http://menandmice,com

DNSSEC Name Resolution

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑



Here is the “delegation signer (DS)” of “org.” + RRSIG

local caching
+ validating
DNS Server

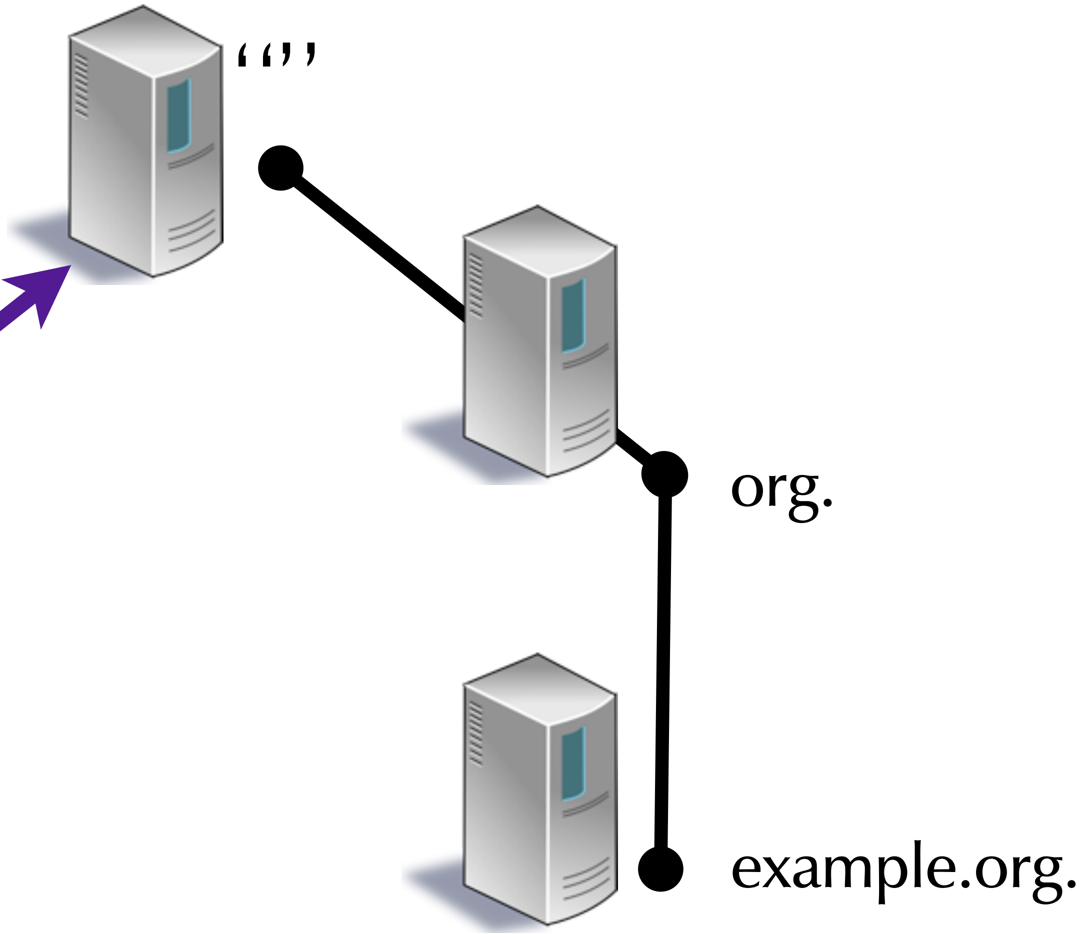
MEN&MICE

© Men & Mice http://menandmice,com

DNSSEC Name Resolution

What is the public key (DNSKEY) of “.”

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑

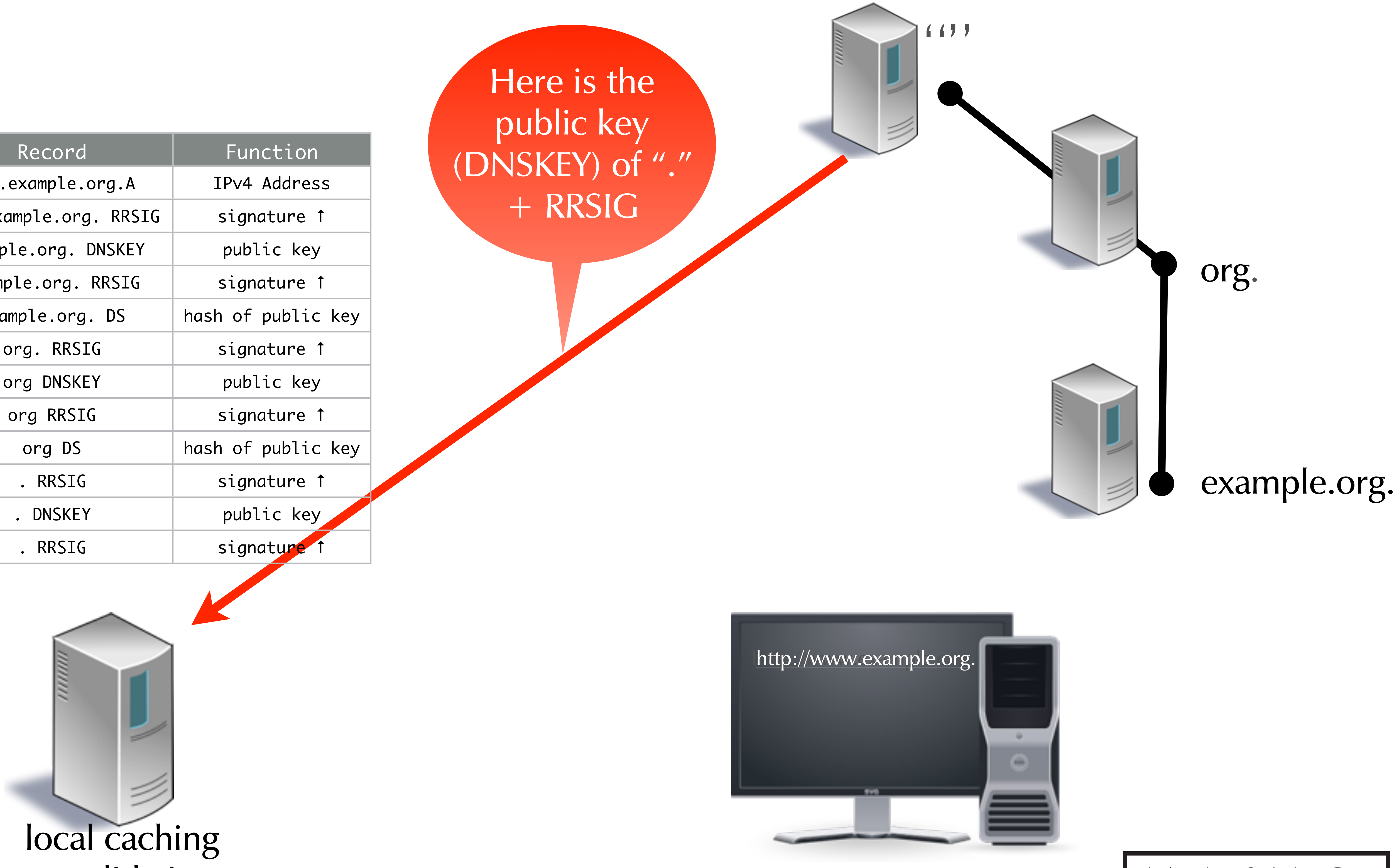


local caching
+ validating
DNS Server

MEN&MICE

© Men & Mice http://menandmice,com

DNSSEC Name Resolution



Here is the public key (DNSKEY) of “.” + RRSIG

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑
. DNSKEY	public key
. RRSIG	signature ↑

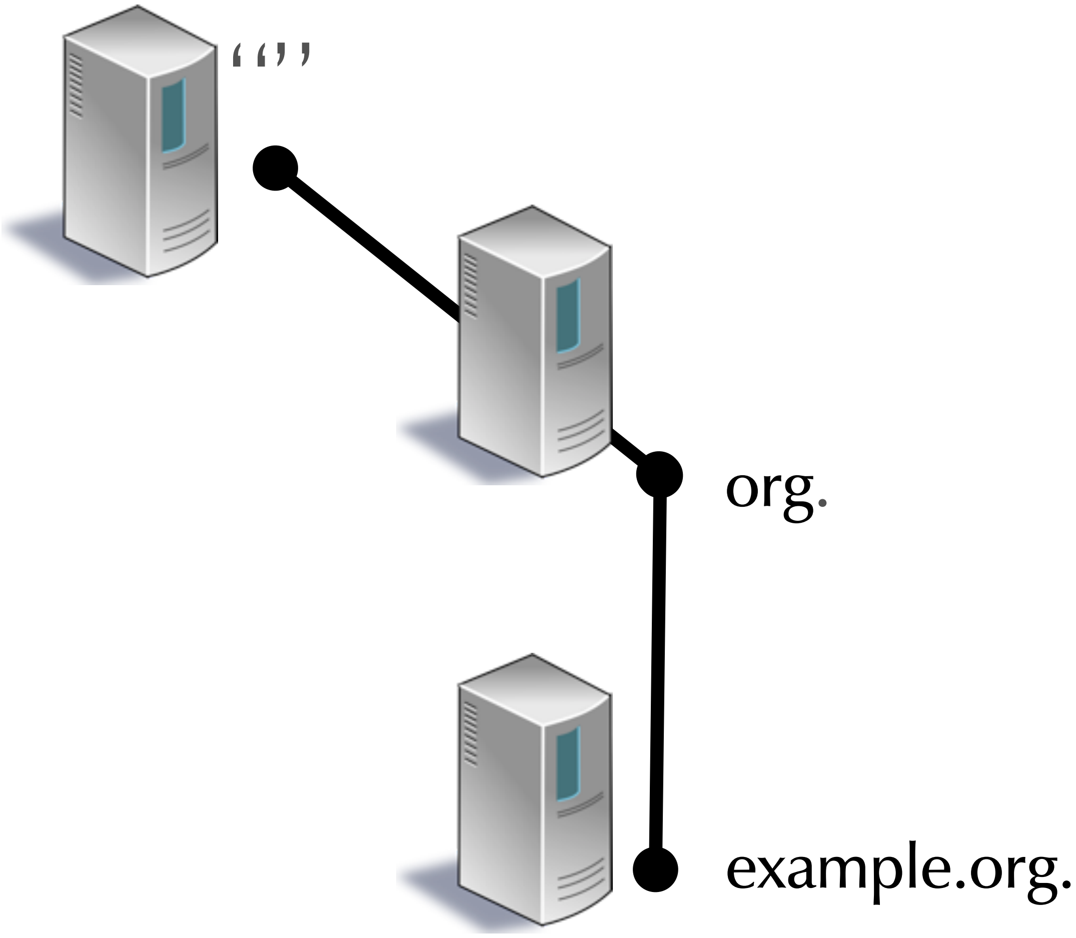
local caching
+ validating
DNS Server

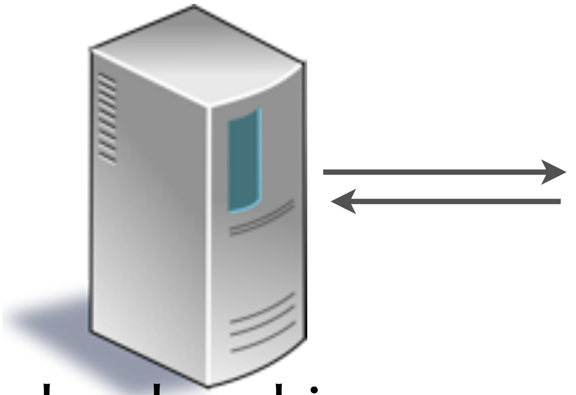
MEN&MICE

© Men & Mice http://menandmice,com

DNSSEC Name Resolution

Record	Function	
www.example.org.A	IPv4 Address	✓
www.example.org. RRSIG	signature ↑	✓
example.org. DNSKEY	public key	✓
example.org. RRSIG	signature ↑	✓
example.org. DS	hash of public key	✓
org. RRSIG	signature ↑	✓
org DNSKEY	public key	✓
org RRSIG	signature ↑	✓
org DS	hash of public key	✓
. RRSIG	signature ↑	✓
. DNSKEY	public key	✓
. RRSIG	signature ↑	✓
Trust Anchor for “.”	hash of public key	





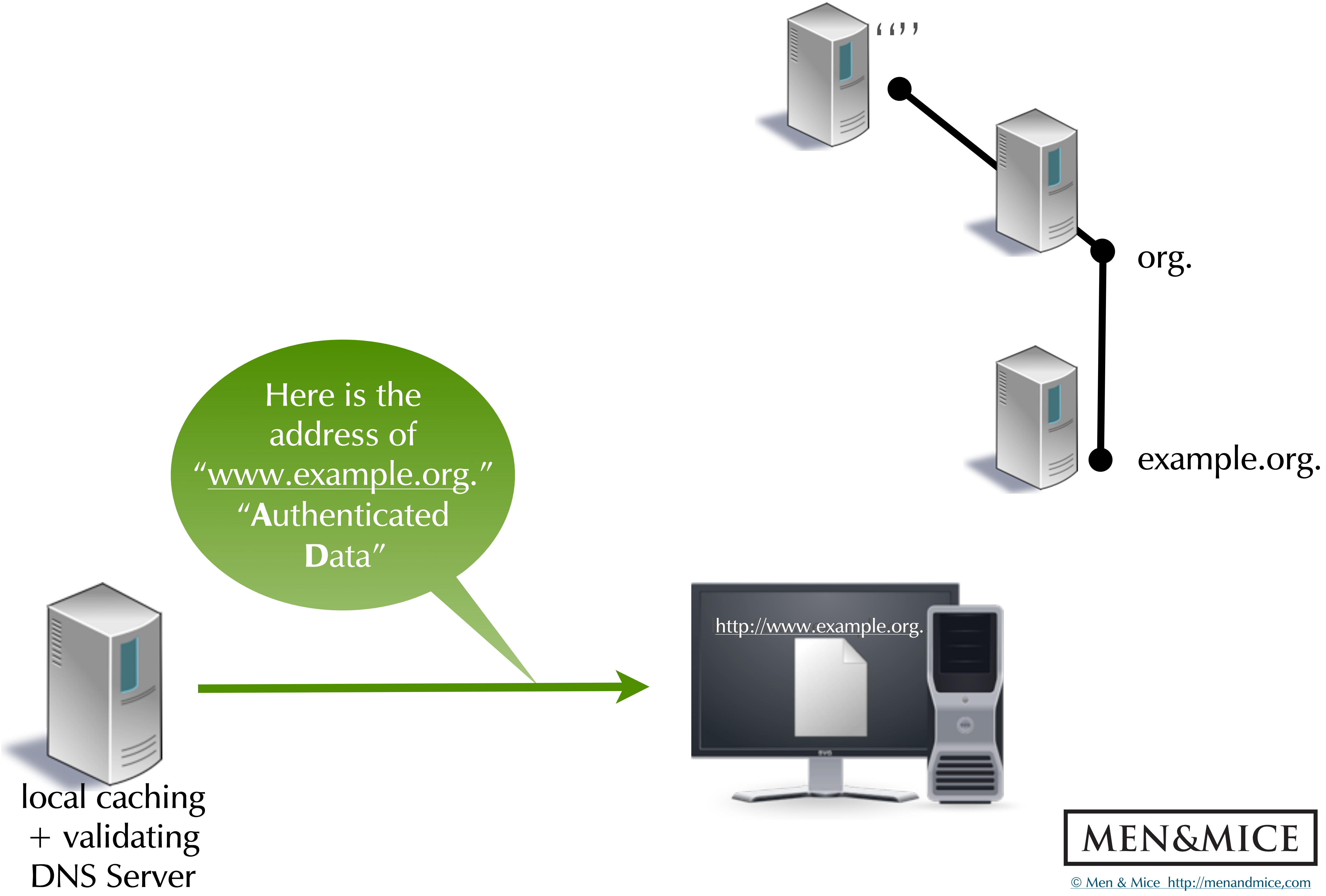
Trush Anchor for “.” (root zone) from configuration file

local caching + validating DNS Server

MEN&MICE

© Men & Mice http://menandmice,com

DNSSEC Name Resolution


"."
org.
example.org.
Here is the address of "www.example.org." "Authenticated Data"
http://www.example.org.
local caching + validating DNS Server

MEN&MICE

© Men & Mice http://menandmice,com

Validation

- the steps on the previous slides are simplified
    - they only show validation on the last DNS query
        - but DNSSEC validation will be done for every query down to the requested domain
    - it only shows validation of one key per zone
        - in reality, we have ZSK and KSK, so twice the amount of checking

DNSSEC aware applications

- Unfortunately, at this time, there is not a validating stub-resolver available
  - The “last hop” is difficult
- Discussion is currently going on regarding the need for standardization

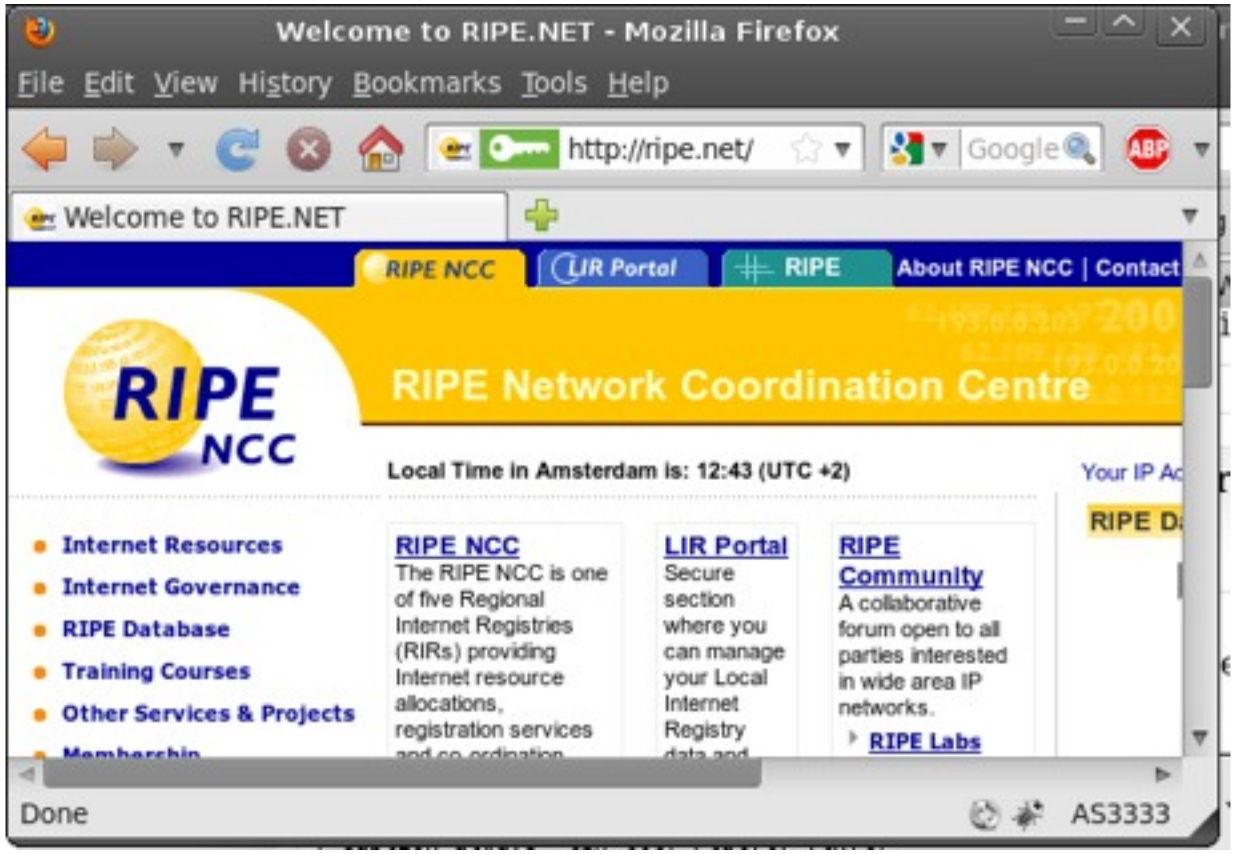
why do we want DNSSEC

- enhanced security
- a common PKI with **one** root trust anchor
  - augment SSL/TLS security (DANE working group)
  - bootstrap key distribution for new Internet services
  - secure key distribution for established Internet services (SSH)

DNSSEC validation in Firefox

- Install the Firefox DNSSEC Add-On (`http://www.dnssec-validator.cz/`)

- and then go to `http://www.root-dnssec.org` or `http://www.ripe.net`



Local Time in Amsterdam is: 12:43 (UTC +2)

RIPE NCC: The RIPE NCC is one of five Regional Internet Registries (RIRs) providing Internet resource allocations, registration services and co-ordination

LIR Portal: Secure section where you can manage your Local Internet Registry data and

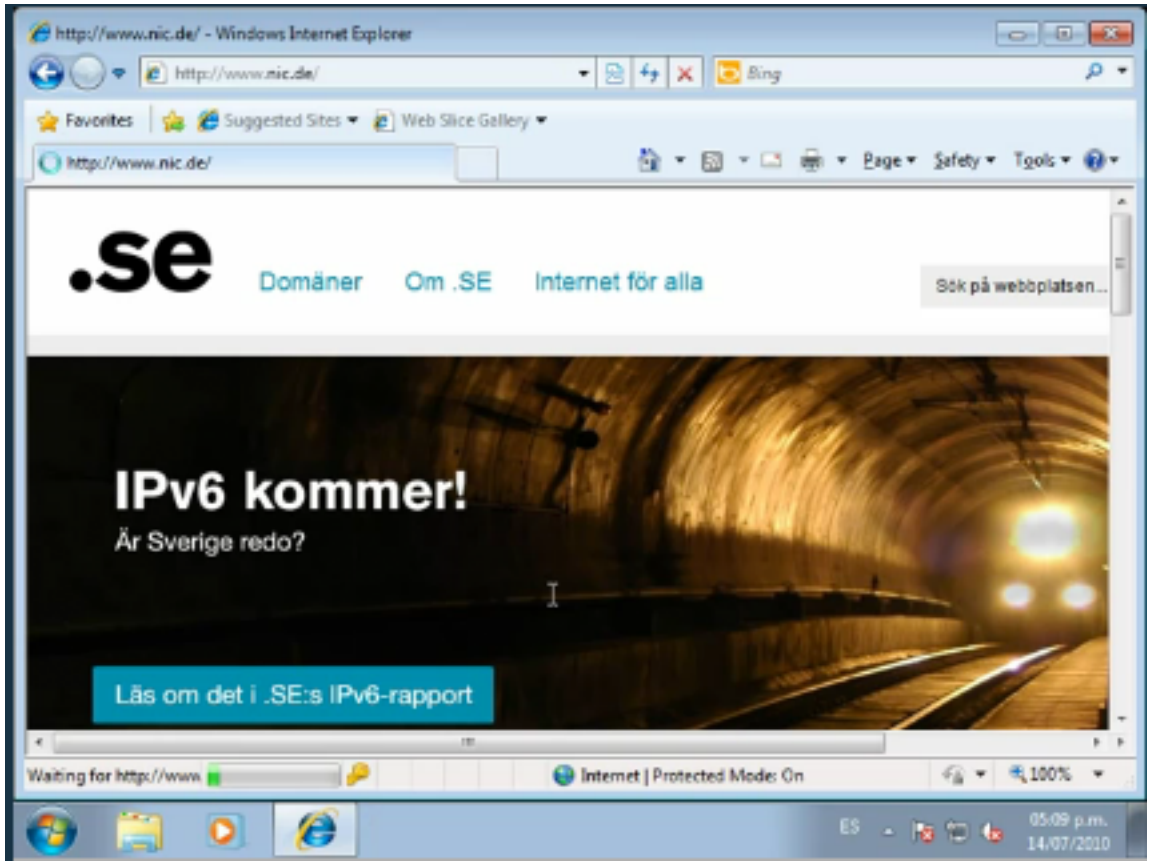
RIPE Community: A collaborative forum open to all parties interested in wide area IP networks.

and you should see a nice green key icon in the URL bar telling you that this DNS information was DNSSEC validated.

© Men & Mice http://menandmice,com

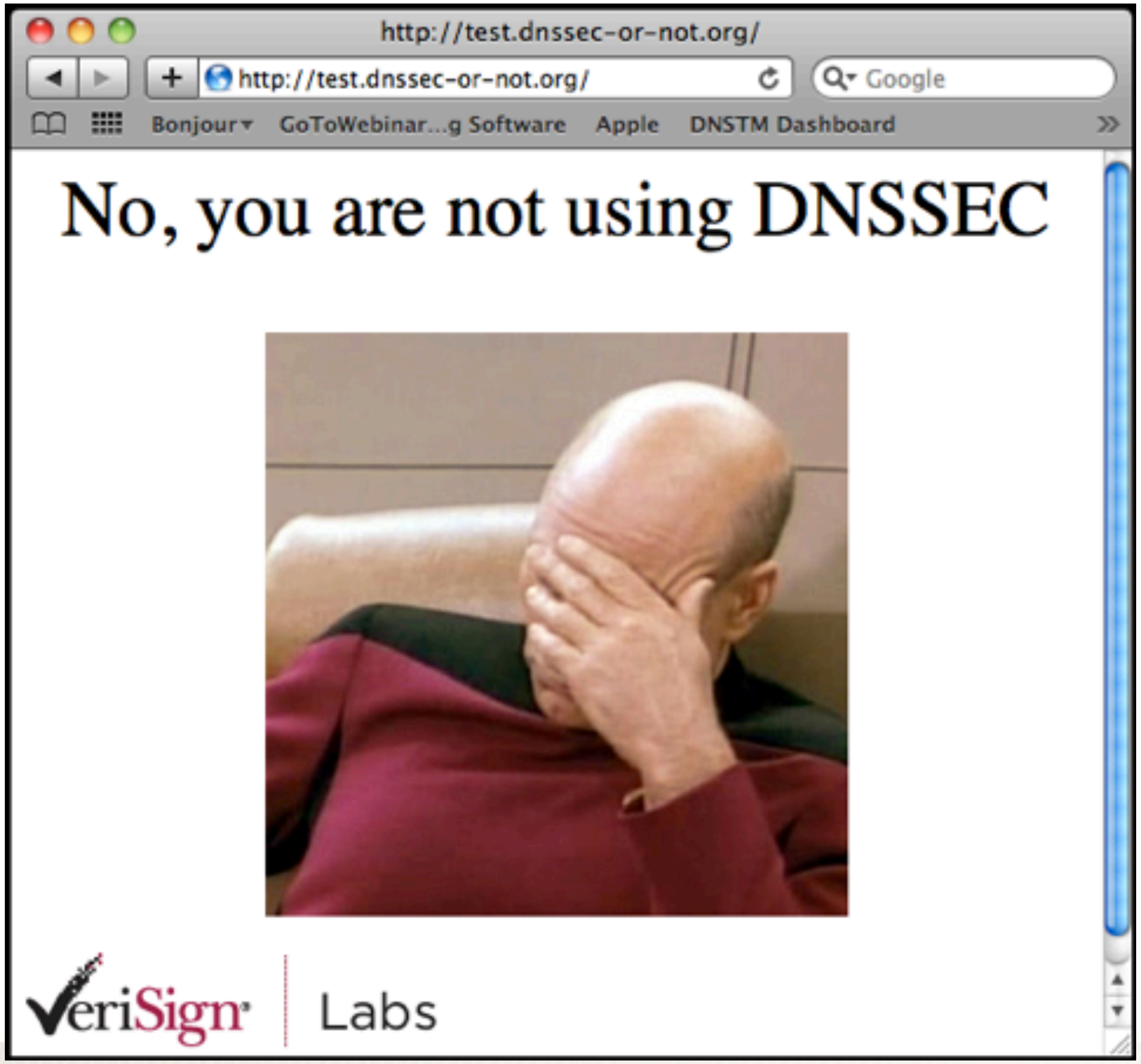
DNSSEC validation in Internet Explorer

- ITESM (Instituto Tecnológico y de Estudios Superiores de Monterrey) and Mexico NIC are providing a DNSSEC plugin tool for the Microsoft Internet Explorer



- http://cs.mty.itesm.mx/dnssecmx/

http://dnssec-or-not.org

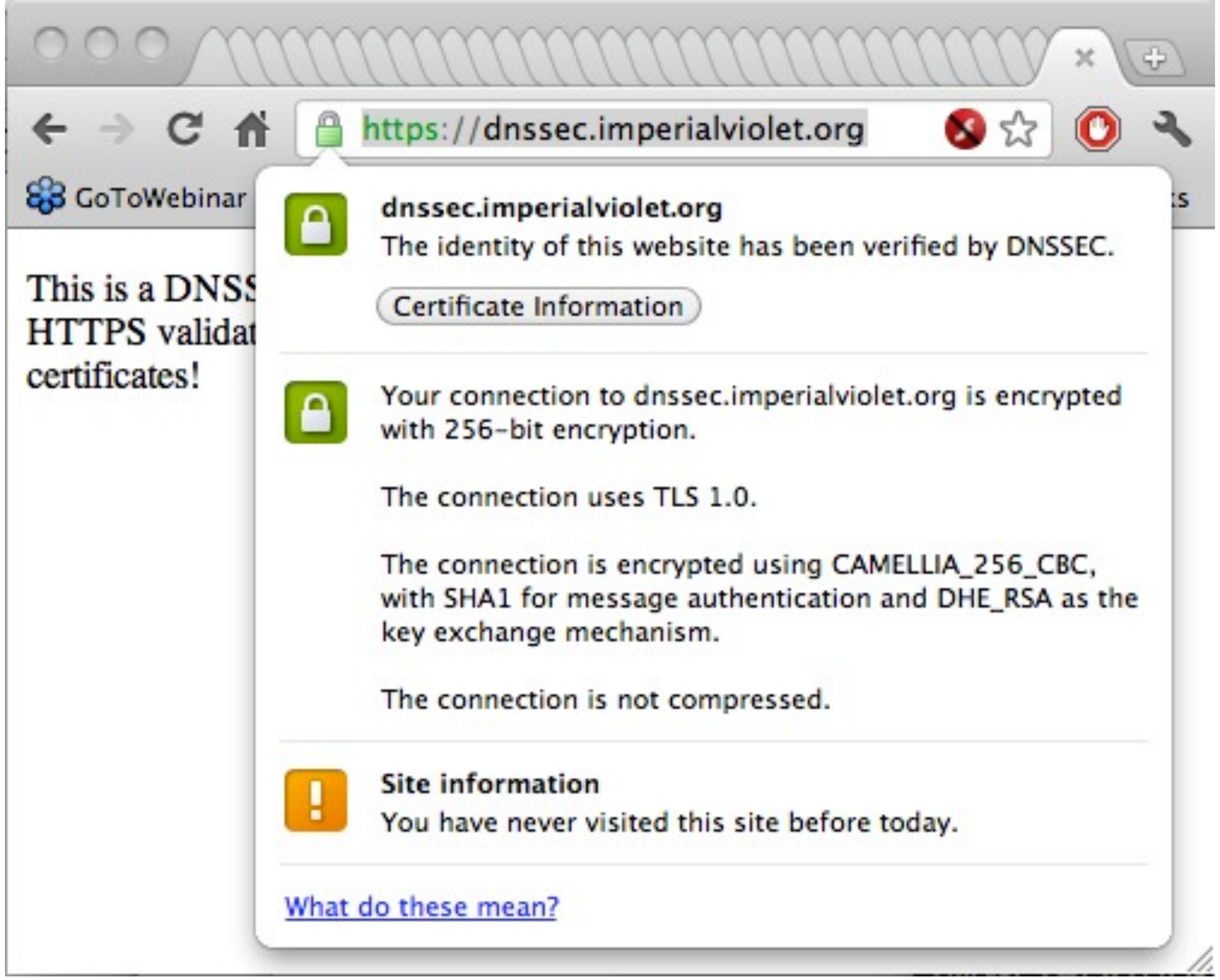


http://test.dnssec-or-not.org/
http://test.dnssec-or-not.org/
Google
Bonjour
GoToWebinar...g Software
Apple
DNSTM Dashboard

No, you are not using DNSSEC

Google Chrome

- As of release 14, the Google Chrome browser supports DNSSEC secured TLS certificates



This is a DNSS
HTTPS validat
certificates!

dnssec.imperialviolet.org
The identity of this website has been verified by DNSSEC.

Your connection to dnssec.imperialviolet.org is encrypted with 256-bit encryption.

The connection uses TLS 1.0.

The connection is encrypted using CAMELLIA_256_CBC, with SHA1 for message authentication and DHE_RSA as the key exchange mechanism.

The connection is not compressed.

Site information
You have never visited this site before today.

© Men & Mice http://menandmice,com

A validating caching configuration for Unbound

Unbound caching server

- Unbound is a dedicated caching DNS Server
  - very limited authoritative functions
  - optimized for caching/resolving only
    - fast and secure

Unbound caching server

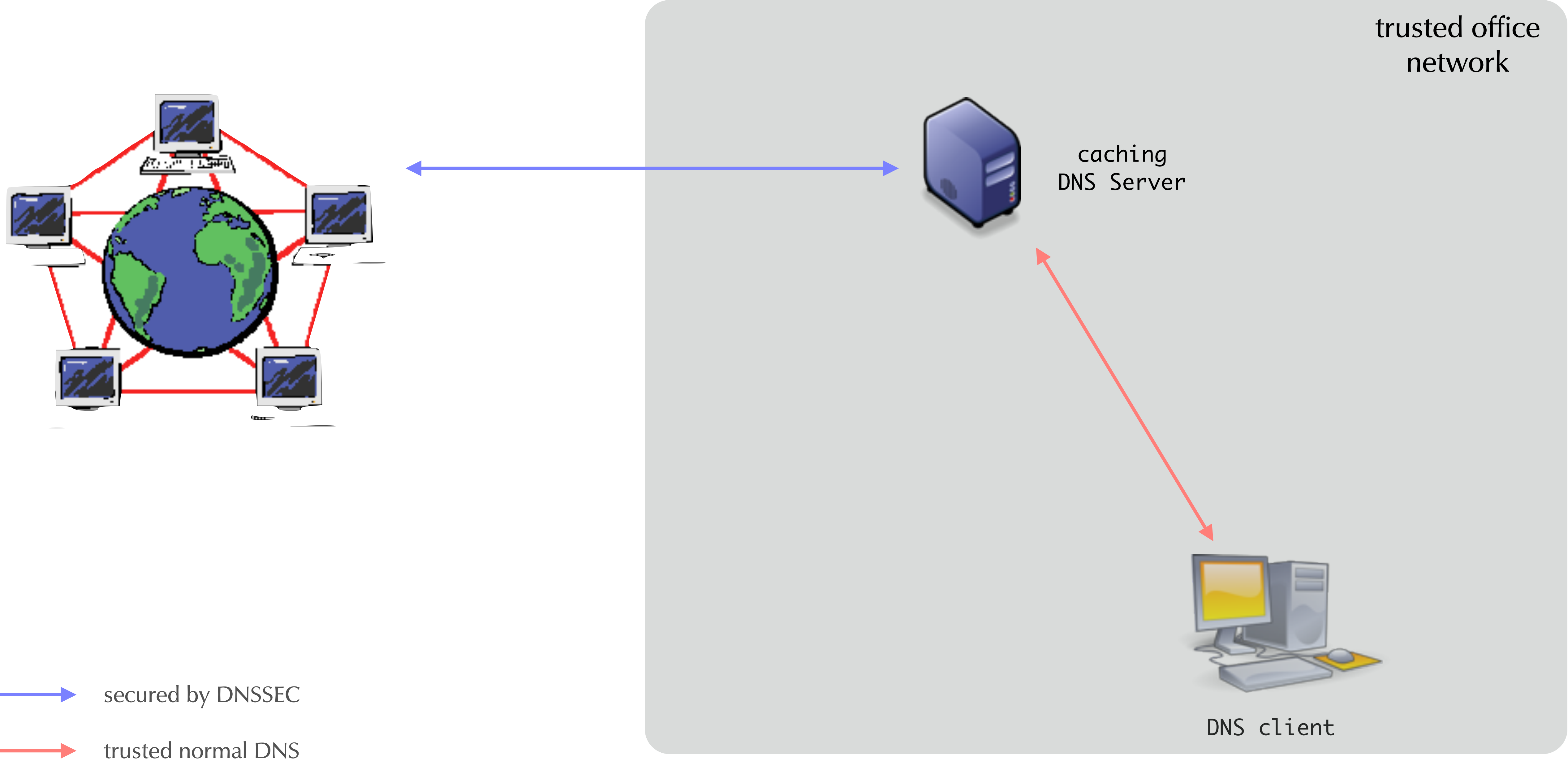
- Unbound is maintained by NlNetLabs
    - http://unbound.net
    - current version: 1.4.16
    - Packages in all major Linux distributions
        - Ubuntu, Debian, SuSE, RedHat/Fedora/CentOS, Gentoo, Arch
        - will be the default DNS server in OpenBSD

DNSSEC-Trigger

the challenge of the last mile

- DNSSEC secures the path between
  - the producer of DNS Data (DNS Admin)
  - a validator, which could be
    - central caching DNS Server
    - an operating system
    - an Application
  - validation should be as close to the point where the data is used

the challenge of the last mile



trusted office network

caching DNS Server

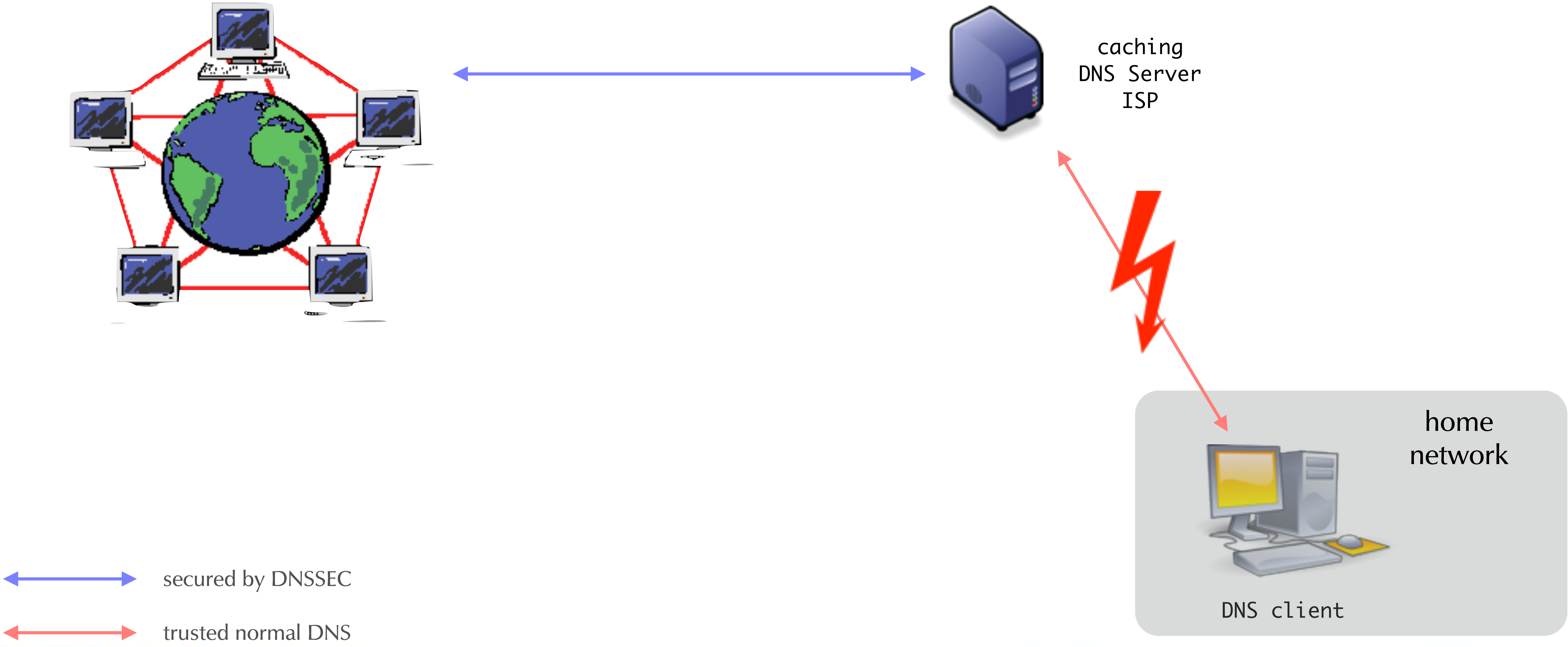
DNS client

↔ secured by DNSSEC

↔ trusted normal DNS

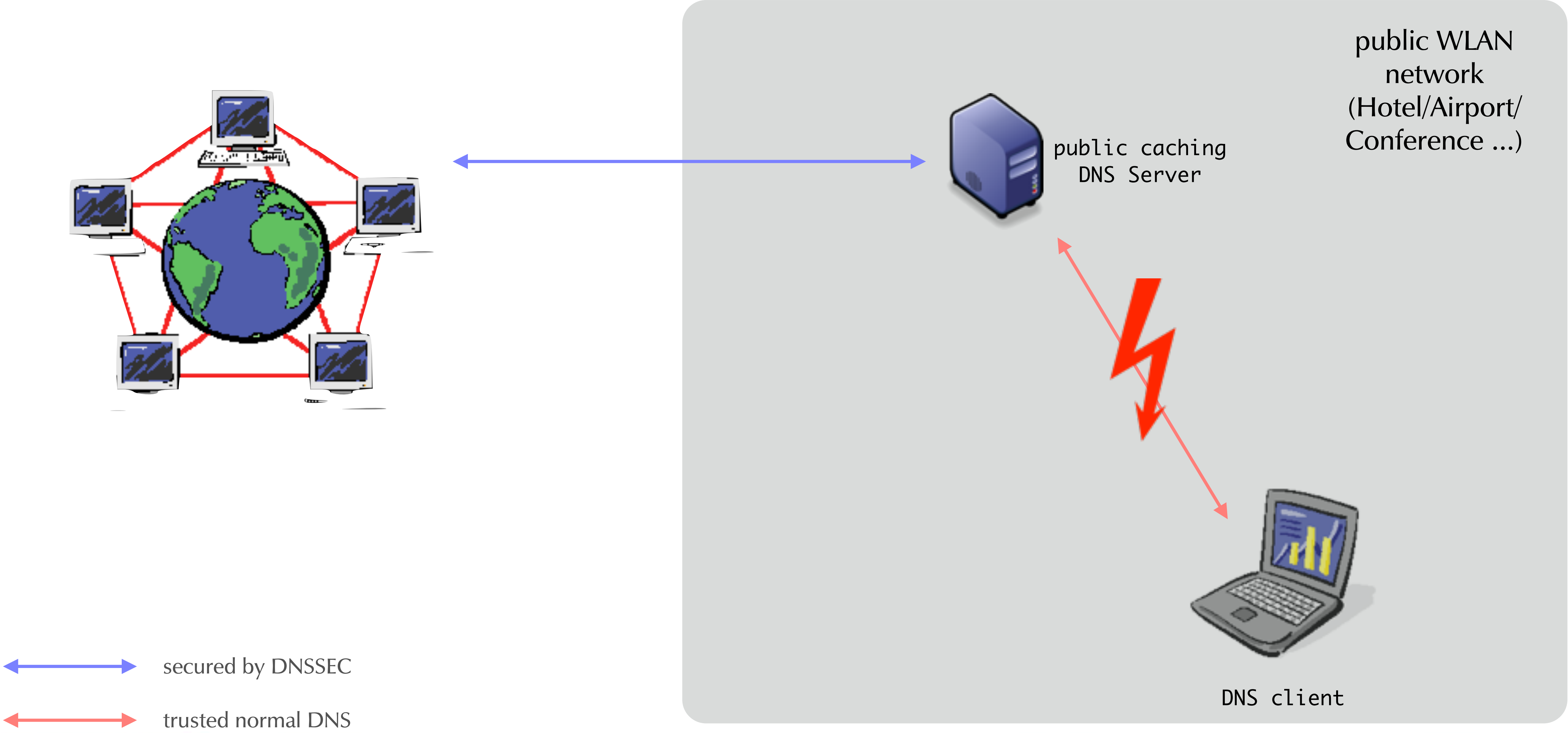
© Men & Mice http://menandmice,com

the challenge of the last mile



© Men & Mice http://menandmice,com

the challenge of the last mile



public WLAN network (Hotel/Airport/ Conference ...)

public caching DNS Server

DNS client

secured by DNSSEC

trusted normal DNS

© Men & Mice http://menandmice,com

solution for the last mile

- a DNSSEC validating DNS Server on my own machine
  - Unbound is a good choice, but ...
- public WLAN systems are notoriously broken
  - strip DNSSEC records
  - no EDNS0 support
  - DNS over TCP blocked
  - violations of the DNS protocol

DNSSEC-Trigger

- a tool to detect brokenness of networks (for DNSSEC)
  - automatically selects the best workaround, if possible
  - allows to go “insecure” for Hotspot-Signon

DNSSEC-Trigger

- DNSSEC-trigger is still work in progress
  - no precompiled-packages for Linux at the moment (Windows and MacOS X packages available)
  - Current version is 0.10
  - `http://www.nlnetlabs.nl/projects/dnssec-trigger/`

DNSSEC-Trigger Installation

MEN&MICE

© Men & Mice http://menandmice,com

step-by-step installation

- Install libdns (LDNS), OpenSSL Header (libssl-dev) and Unbound
  - using the systems package manager
  - or download from `http://support.menandmice.com/download/unbound` and `http://support.menandmice.com/download/ldns`

step-by-step installation

- if another DNS server is already running on port 53, it must be disabled
  - Ubuntu 12.04 has “dnsmasq” running by default, it can be disabled in `/etc/NetworkManager/Networkmanager.conf`

step-by-step installation

- make sure Unbound is running ...

```
# ps -ef | grep unbound
```

- make sure Unbound can resolve DNS queries

```
# drill @localhost www.luga.de
```

step-by-step installation

- make sure we can remote control Unbound ...
  # sudo `unbound-control status`

- fetch the DNSSEC public key for the root DNS zone
  ```
  # sudo unbound-anchor -v
  ```

step-by-step installation

- verify the DNSSEC root key ...

```
# cat /etc/unbound/root.key
; autotrust trust anchor file
;;id: . 1
;;last_queried: 1332424921 ;;Thu Mar 22 15:02:01 2012
;;last_success: 1332424921 ;;Thu Mar 22 15:02:01 2012
;;next_probe_time: 1332464202 ;;Fri Mar 23 01:56:42 2012
;;query_failed: 0
;;query_interval: 43200
;;retry_time: 8640
.      172800   IN   DNSKEY   257 3 8 AwEAAagAIKlVZrpC6Ia7gEzahOR
+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/
RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/
Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hOA2hzCTMjJPJ8LbqF6dsV
6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu
+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0= ;{id = 19036 (ksk), size
= 2048b} ;;state=2 [  VALID  ] ;;count=0 ;;lastchange=1323870465 ;;Wed Dec 14 14:47:45
2011
```

step-by-step installation

- verify that Unbound does DNSSEC validation ...

```
# drill -D www.ripe.net @localhost
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 46801
;; flags: qr rd ra ad ; QUERY: 1, ANSWER: 2, AUTHORITY: 7, ADDITIONAL: 4
;; QUESTION SECTION:
;; www.ripe.net.    IN    A

;; ANSWER SECTION:
www.ripe.net. 21581 IN    A     193.0.6.139
www.ripe.net. 21581 IN    RRSIG A 5 3 21600 20120421100055 20120322090055 8823 ripe.net.
O44UGpuxl8rVnr2SLJ01ngygDvE6oEqZGM3S55sonQ1A4FFfoJSOrvfHsss2LrHtaimO52C3sgAmubJEhwv4/iR/lAD64/bmh9DC8aD/In
+CIxFZ+a7KneKgpGTNFHM6Ghu6v/T5RKMZzhaswdKE3VGAQAhbwE4c0Ytxm5auxu4=
[....]
```

step-by-step installation

- download the DNSSEC-Trigger source ...

```
# wget http://www.nlnetlabs.nl/downloads/dnssec-trigger/dnssec-trigger-0.10.tar.gz
```

step-by-step installation

- install dependencies (libgtk-dev/libgtk2.0-dev, libglib-dev/libglib2.0-dev, libldns-dev)
- build DNSSEC-Trigger from source ...

```
# tar xfz dnssec-trigger-0.10.tar.gz
# cd dnssec-trigger-0.10
# ./configure
# make
# sudo make install
```

© Men & Mice http://menandmice,com

step-by-step installation

- create cryptographic keys to be able to control the dnssec-triggerd process:

```
# sudo dnssec-trigger-control-setup
```

step-by-step installation

- create cryptographic keys to be able to control the dnssec-triggerd process:

```
# sudo dnssec-trigger-control-setup
```

step-by-step installation

- manually start dnssec-trigger daemon:

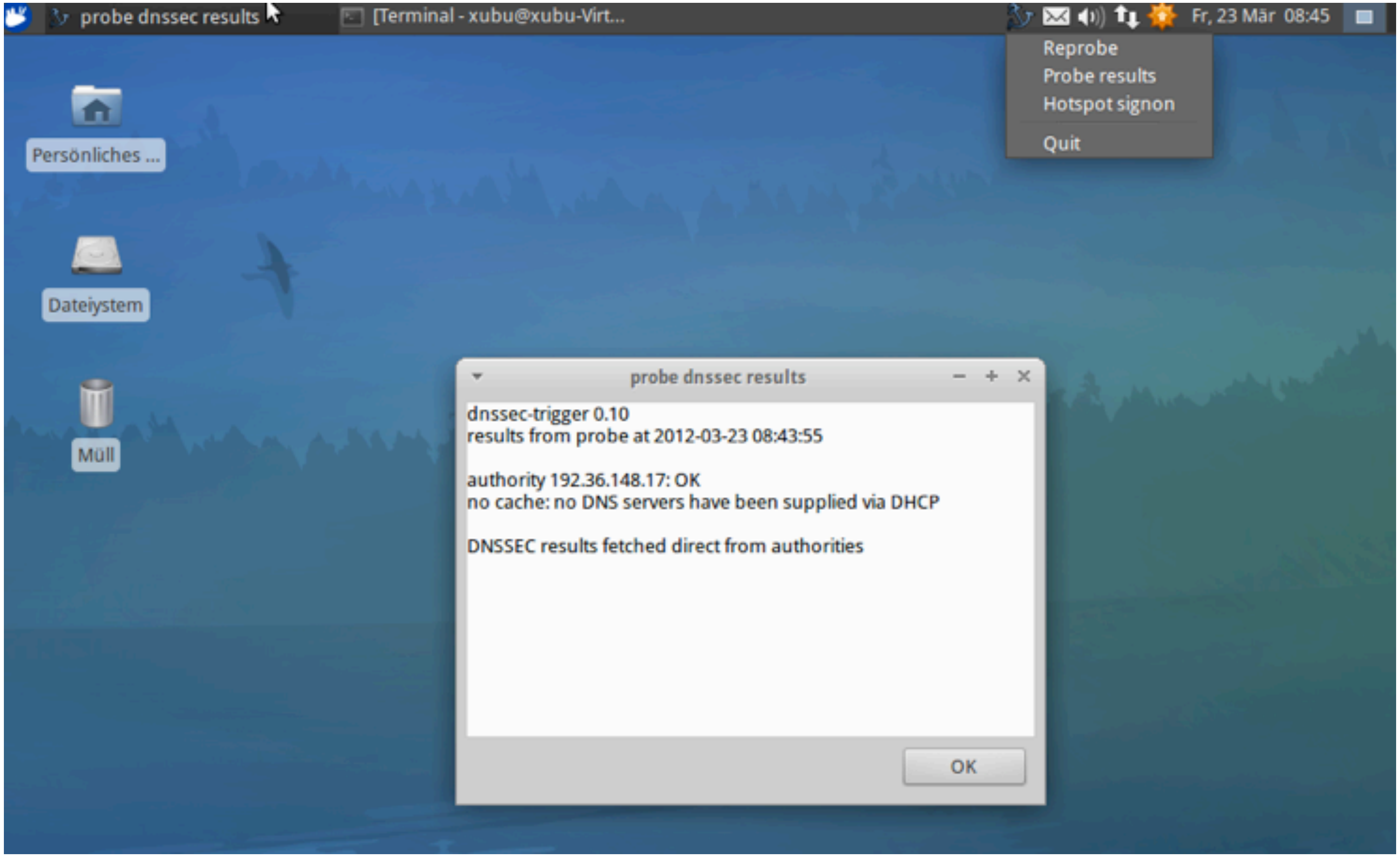
```
# sudo /usr/local/sbin/dnssec-triggerd
```

step-by-step installation

- manually start dnssec-trigger panel:

```
# /usr/local/bin/dnssec-trigger-panel
```

step-by-step installation



```
dnssec-trigger 0.10
results from probe at 2012-03-23 08:43:55

authority 192.36.148.17: OK
no cache: no DNS servers have been supplied via DHCP

DNSSEC results fetched direct from authorities
```

© Men & Mice http://menandmice,com

step-by-step installation

- test DNSSEC and dnssec-trigger:

```
# sudo dnssec-trigger-control reprobe
# sudo dnssec-trigger-control status
# drill -D @localhost ripe.net
```

step-by-step installation

- if it works, write a start-script (or systemd/upstartd config) for dnssec-triggerd
- there is an example from Fedora Linux in the “fedora” directory in the source tree

DNSSEC-Trigger troubleshooting

troubleshooting

- check that dnssec-triggerd and Unbound are running

```
# ps -ef | grep unbound

# ps -ef | grep dnssec-triggerd
```

troubleshooting

- local resolver configuration should point only to local machine

```
# cat /etc/resolv.conf
search .
nameserver 127.0.0.1
```

troubleshooting

- check Unbound forward configuration (here DNS queries will be forwarded to a DNS server at 192.168.1.2)

```
# unbound-control forward
192.168.1.2
```

© Men & Mice http://menandmice,com

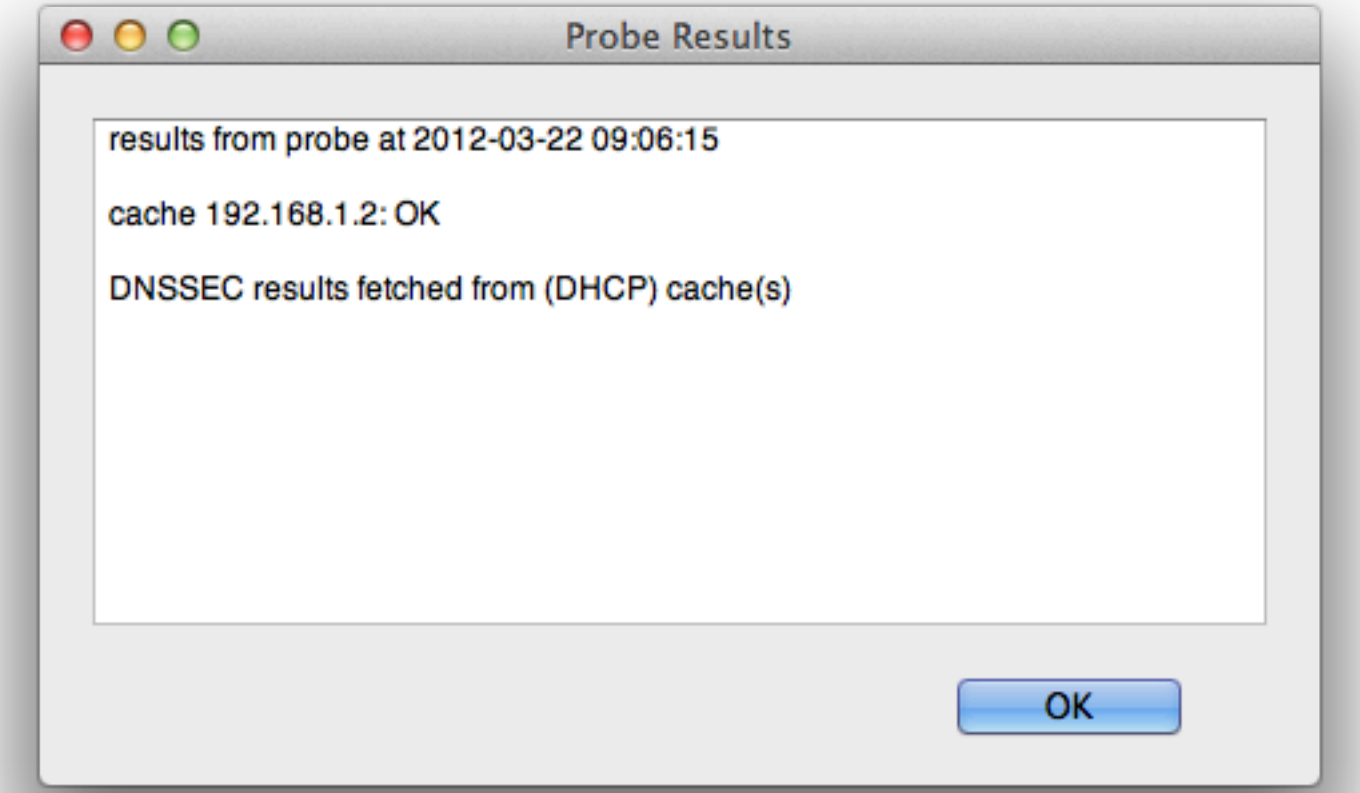
troubleshooting

- check DNSSEC-Trigger status

```
# dnssec-trigger-control status
at 2012-03-22 09:06:15
cache 192.168.1.2: OK
state: cache secure
```

troubleshooting

- check DNSSEC-Trigger status via panel applet



```
results from probe at 2012-03-22 09:06:15

cache 192.168.1.2: OK

DNSSEC results fetched from (DHCP) cache(s)
```

© Men & Mice http://menandmice,com

troubleshooting

- in Hot-Spot WLAN, go insecure during signon if needed:

```
# dnssec-trigger-control hotspot_signon

# dnssec-trigger-control status
at 2012-03-22 09:06:15
cache 192.168.1.2: OK
state: nodnssec forced_insecure
```

© Men & Mice http://menandmice,com

troubleshooting

- don’t forget to “reprobe” after sign-on to get security again

```
# dnssec-trigger-control reprobe
```

troubleshooting

- to override the set of DNS servers to use

```
# dnssec-trigger-control submit 94.75.228.29 62.141.58.13
```

- Google public DNS server (8.8.8.8 and 8.8.4.4) do not support DNSSEC at the moment (March 2012)!
  - DNS Server above are from the German Privacy Foundation and Swiss Privacy Foundation (`http://server.privacyfoundation.de/`)

troubleshooting

- check the AD-Flag in requests from time to time

```
# drill -D ripe.net
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 8717
;; flags: qr rd ra ad ; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; ripe.net.	IN	A

;; ANSWER SECTION:
ripe.net.	21600	IN	A	193.0.6.139
ripe.net.	21600	IN	RRSIG A 5 2 21600 20120421151506 20120322141506 8823 ripe.net.
fm28MCVltrVdfhSK3TKJoNqlQFsJuF9aY7KQQOW+G0CsJG9E9rhWykRg1Gu4NbEUEtu6Yao/JFgKSD1mlQRuxWcD3nVwrH7saoOdcA
+oFVpqEYIm3J8bombWZR7G749TvAX00I/oZIVYvzmNki+RVfNxXfhOH5TKt+6ufOgjk5w=

;; AUTHORITY SECTION:

;; ADDITIONAL SECTION:

;; Query time: 319 msec
;; EDNS: version 0; flags: do ; udp: 4096
;; SERVER: 127.0.0.1
;; WHEN: Thu Mar 22 19:41:54 2012
;; MSG SIZE  rcvd: 221
```

© Men & Mice http://menandmice,com

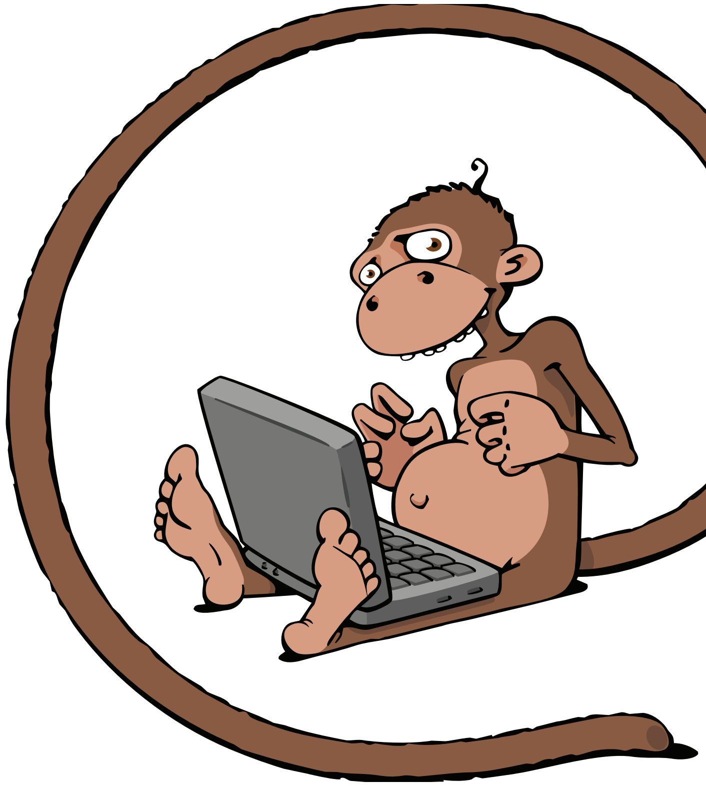
DNSSEC-Trigger deinstallation

deinstallation

- if you need to de-install dnssec-trigger, run:

```
# sudo dnssec-trigger-control-setup -u
```

- remove the startup script (or configuration) for dnssec-triggerd
- and kill the dnssec-triggerd process if it is running



Thank you!

E-Mail:
carsten@menandmice.com
more on DNSSEC: `http://www.linuxhotel.de/kurs/dnssec/`

MEN&MICE