DNS Security

Chun-Jen (James) Chung

Arizona State University

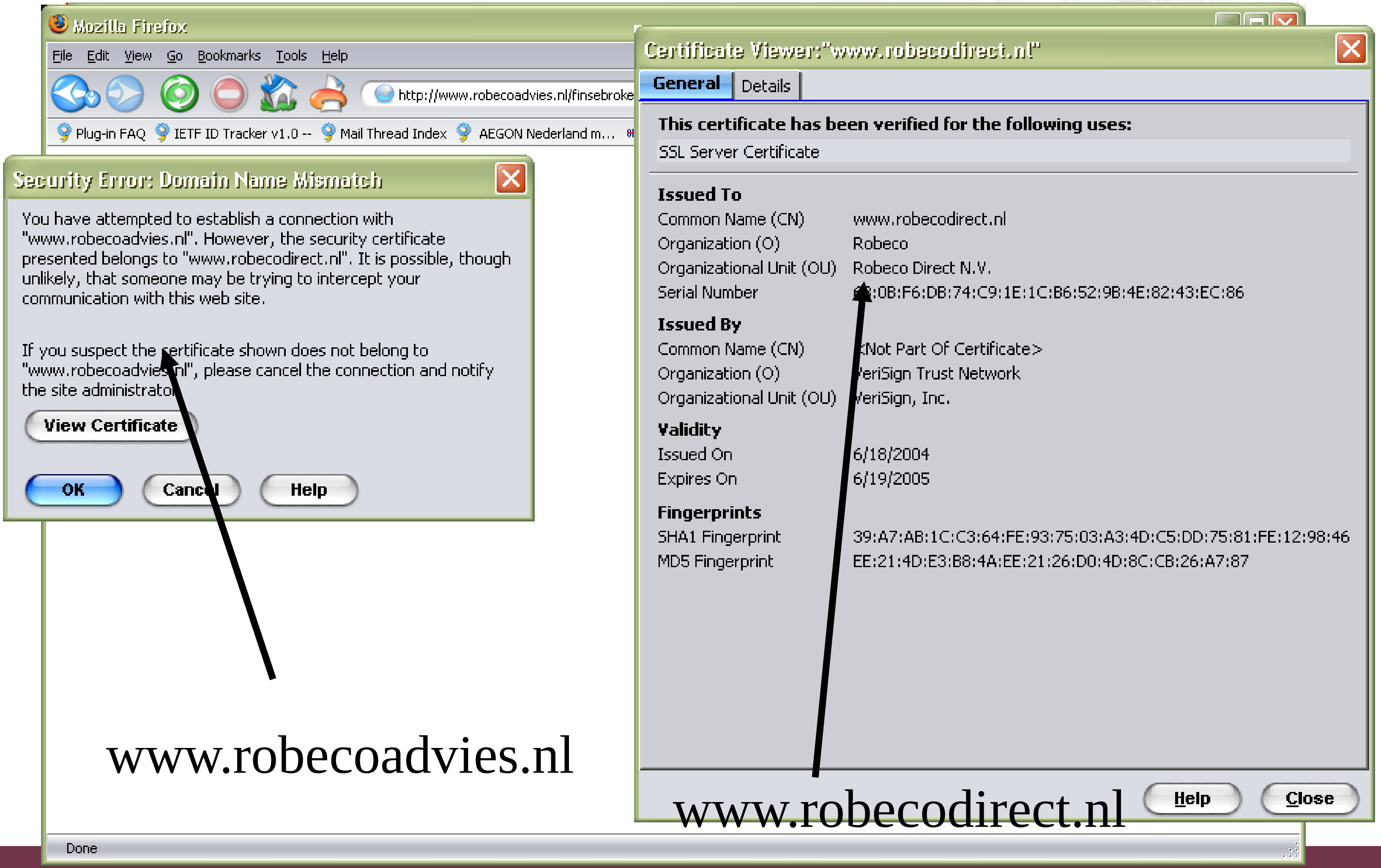
DNS Known Concepts

- Known DNS concepts:
  - Delegation, Referral, Zone, RRs, label, RDATA, Authoritative server, caching forwarder, resolver, SOA parameters

Why DNSSEC

- Good security is multi-layered and preventive
  - Multiple defense barriers in physical world
  - Multiple ‘layers’ in the networking world
- DNS infrastructure
  - Providing DNSSEC extensions to raise the barrier for DNS based attacks
  - Provides a security barrier or an enhancement for systems and applications

Example 1: mismatched CN



Security Error: Domain Name Mismatch

You have attempted to establish a connection with "www.robecoadvies.nl". However, the security certificate presented belongs to "www.robecodirect.nl". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.

If you suspect the certificate shown does not belong to "www.robecoadvies.nl", please cancel the connection and notify the site administrator.

Certificate Viewer:"www.robecodirect.nl"

This certificate has been verified for the following uses:

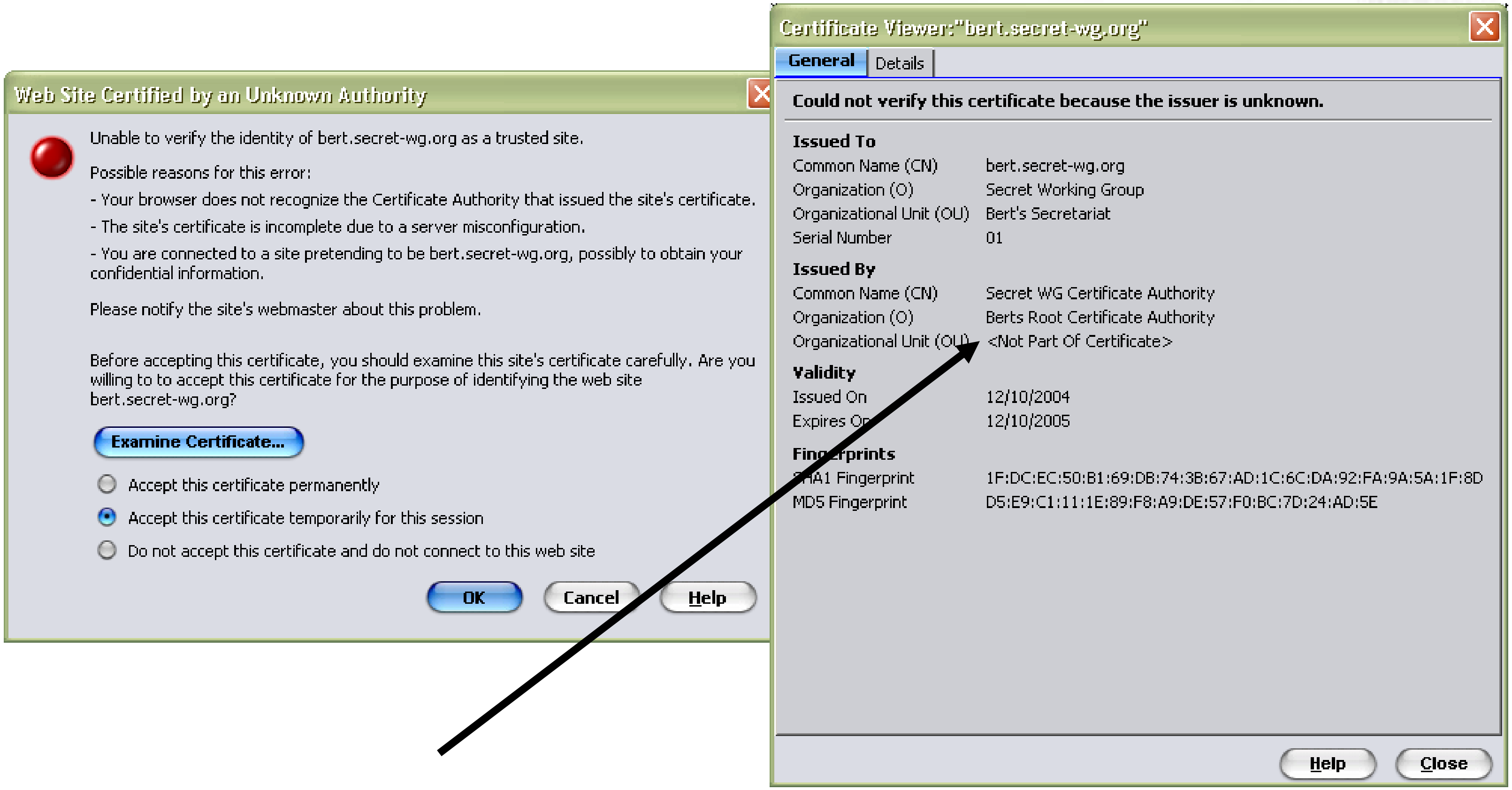
SSL Server Certificate

Issued To	
Common Name (CN)	www.robecodirect.nl
Organization (O)	Robeco
Organizational Unit (OU)	Robeco Direct N.V.
Serial Number	6B:0B:F6:DB:74:C9:1E:1C:B6:52:9B:4E:82:43:EC:86
Issued By	
Common Name (CN)	<Not Part Of Certificate>
Organization (O)	VeriSign Trust Network
Organizational Unit (OU)	VeriSign, Inc.
Validity	
Issued On	6/18/2004
Expires On	6/19/2005
Fingerprints	
SHA1 Fingerprint	39:A7:AB:1C:C3:64:FE:93:75:03:A3:4D:C5:DD:75:81:FE:12:98:46
MD5 Fingerprint	EE:21:4D:E3:B8:4A:EE:21:26:D0:4D:8C:CB:26:A7:87

www.robecoadvies.nl

www.robecodirect.nl

Example 2: Unknown CA



Web Site Certified by an Unknown Authority

Unable to verify the identity of bert.secret-wg.org as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be bert.secret-wg.org, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the web site bert.secret-wg.org?

○ Accept this certificate permanently

● Accept this certificate temporarily for this session

○ Do not accept this certificate and do not connect to this web site

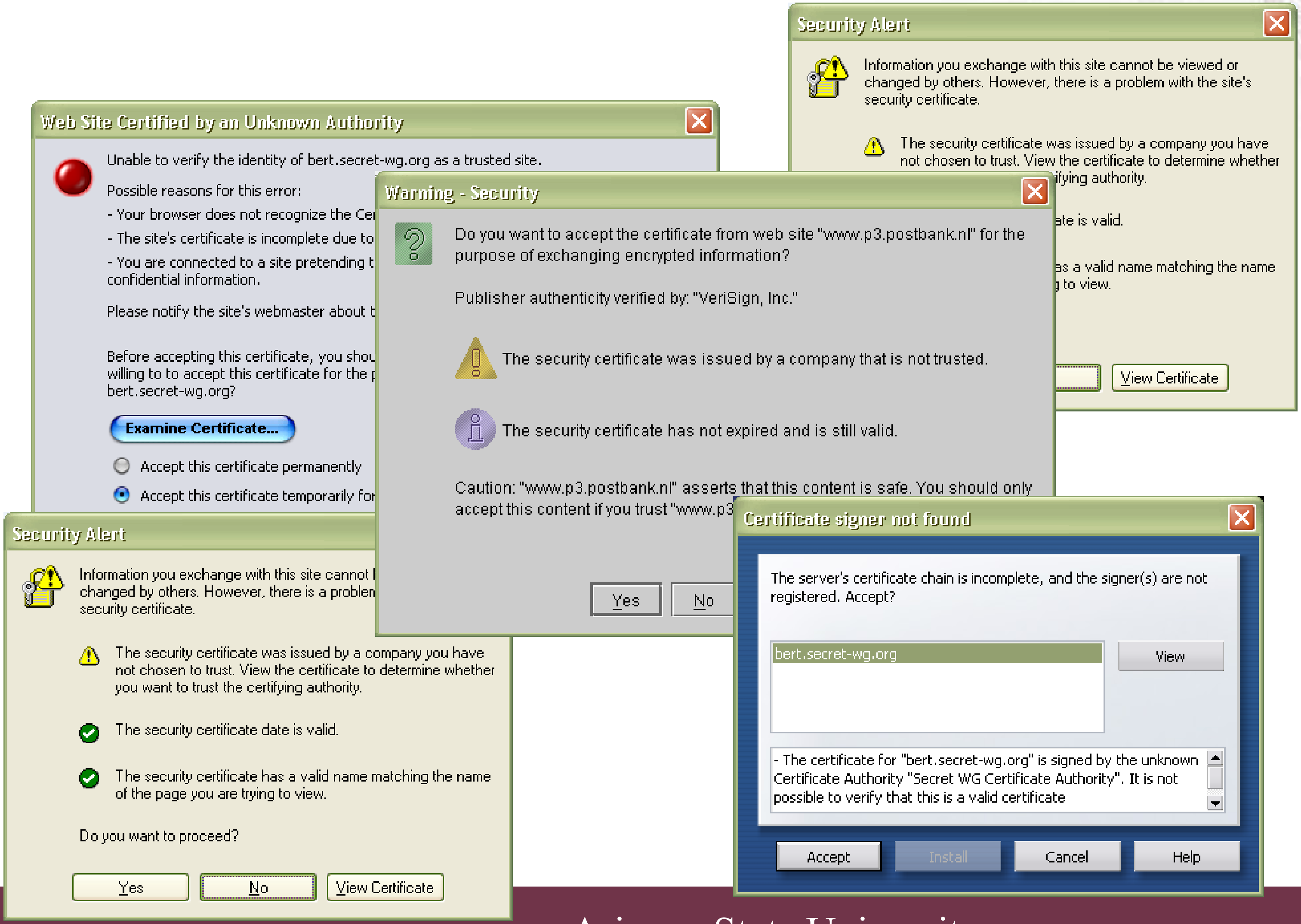
Certificate Viewer:"bert.secret-wg.org"

Could not verify this certificate because the issuer is unknown.

Issued To	
Common Name (CN)	bert.secret-wg.org
Organization (O)	Secret Working Group
Organizational Unit (OU)	Bert's Secretariat
Serial Number	01
Issued By	
Common Name (CN)	Secret WG Certificate Authority
Organization (O)	Berts Root Certificate Authority
Organizational Unit (OU)	<Not Part Of Certificate>
Validity	
Issued On	12/10/2004
Expires On	12/10/2005
Fingerprints	
SHA1 Fingerprint	1F:DC:EC:50:B1:69:DB:74:3B:67:AD:1C:6C:DA:92:FA:9A:5A:1F:8D
MD5 Fingerprint	D5:E9:C1:11:1E:89:F8:A9:DE:57:F0:BC:7D:24:AD:5E

Unknown Certificate Authority

Confused?



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether …ifying authority.

…ate is valid.

…as a valid name matching the name …g to view.

Web Site Certified by an Unknown Authority

Unable to verify the identity of bert.secret-wg.org as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Cer…
- The site's certificate is incomplete due to…
- You are connected to a site pretending t… confidential information.

Please notify the site's webmaster about t…

Before accepting this certificate, you shou… willing to to accept this certificate for the p… bert.secret-wg.org?

○ Accept this certificate permanently

● Accept this certificate temporarily for…

Warning - Security

Do you want to accept the certificate from web site "www.p3.postbank.nl" for the purpose of exchanging encrypted information?

Publisher authenticity verified by: "VeriSign, Inc."

The security certificate was issued by a company that is not trusted.

The security certificate has not expired and is still valid.

Caution: "www.p3.postbank.nl" asserts that this content is safe. You should only accept this content if you trust "www.p3…

Security Alert

Information you exchange with this site cannot b… changed by others. However, there is a problem… security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

✓ The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

Certificate signer not found

The server's certificate chain is incomplete, and the signer(s) are not registered. Accept?

bert.secret-wg.org

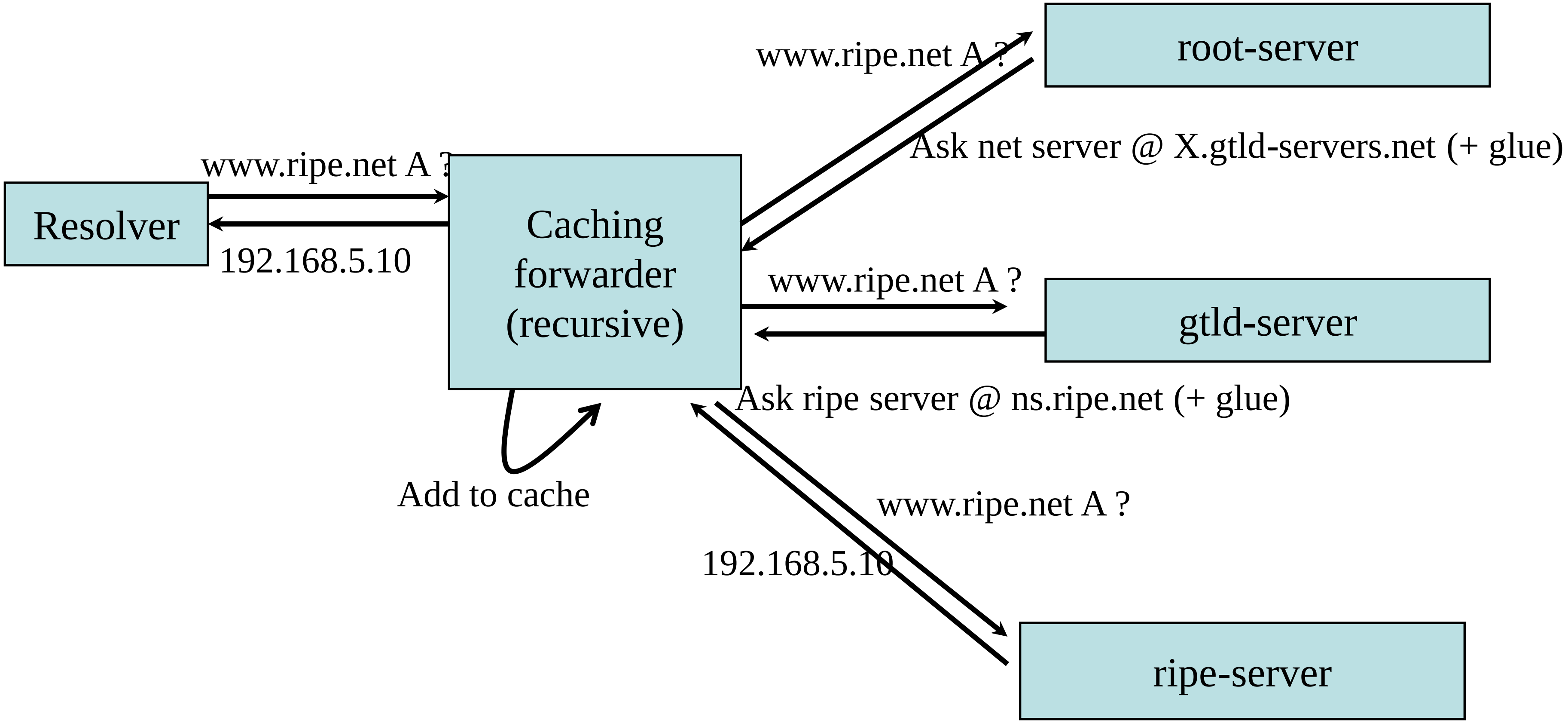
- The certificate for "bert.secret-wg.org" is signed by the unknown Certificate Authority "Secret WG Certificate Authority". It is not possible to verify that this is a valid certificate

How does DNSSEC come into this picture?

- DNSSEC secures the name to address mapping
  - before the certificates are needed
- 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?”

DNS resolving

Question: www.ripe.net A



root-server

www.ripe.net A ?

Ask net server @ X.gtld-servers.net (+ glue)

Resolver

www.ripe.net A ?

192.168.5.10

Caching forwarder (recursive)

www.ripe.net A ?

gtld-server

Ask ripe server @ ns.ripe.net (+ glue)

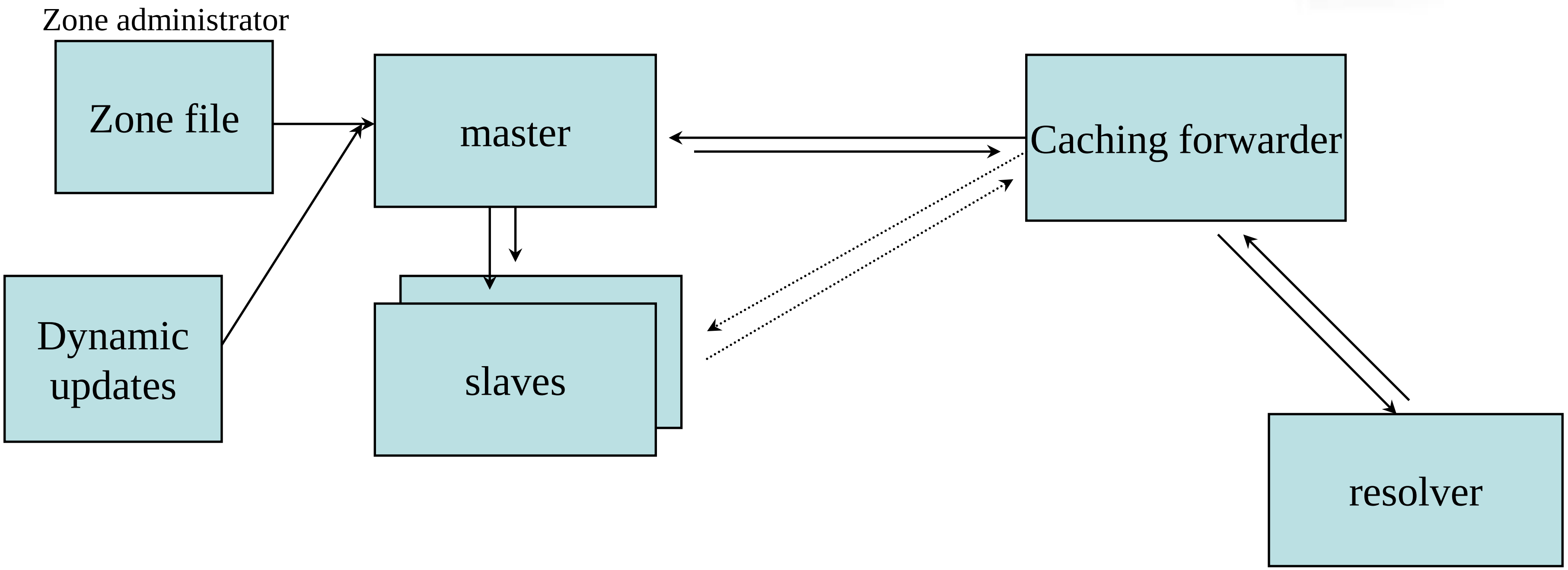
Add to cache

www.ripe.net A ?

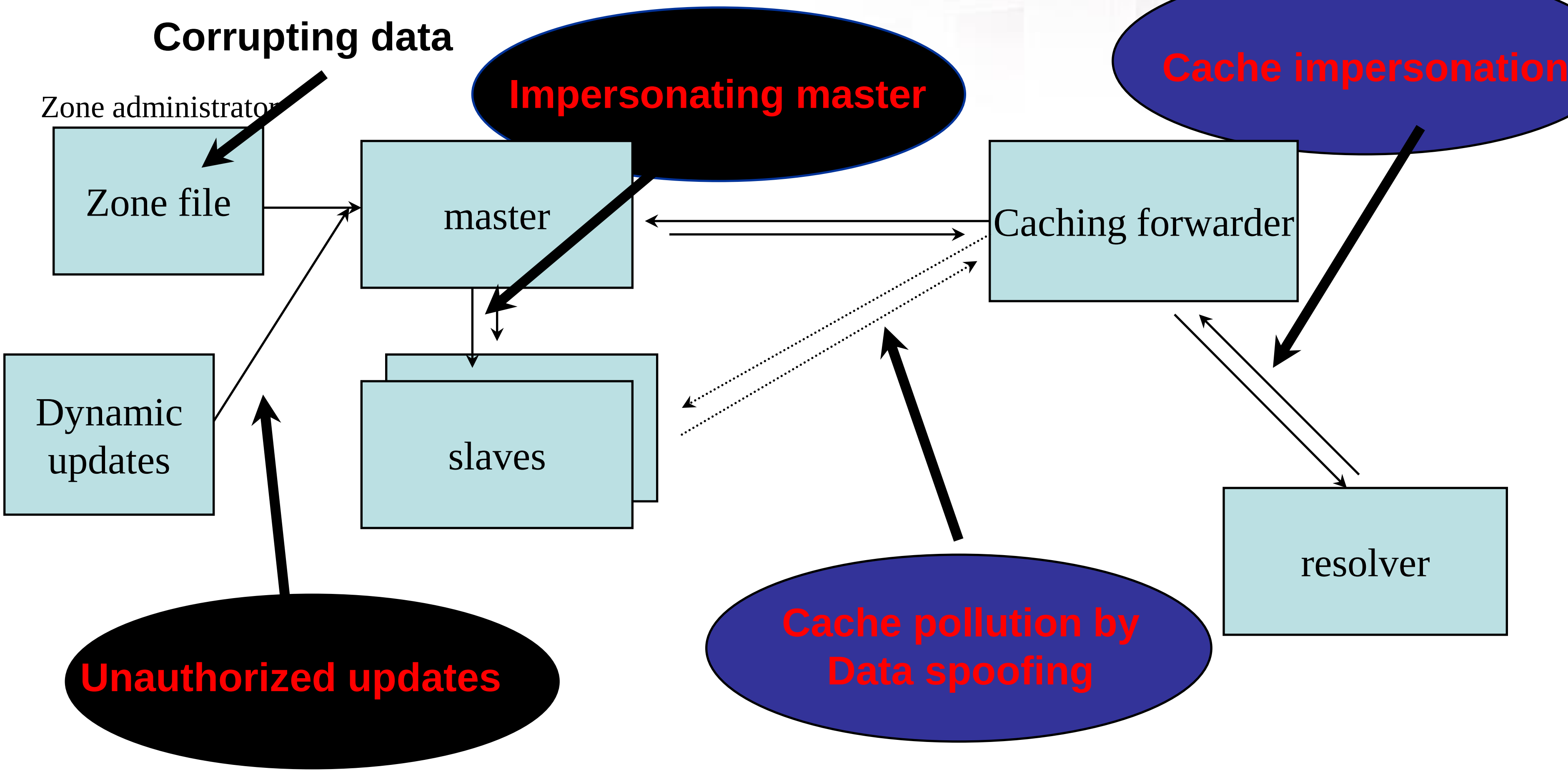
192.168.5.10

ripe-server

DNS Data flow



DNS Vulnerabilities



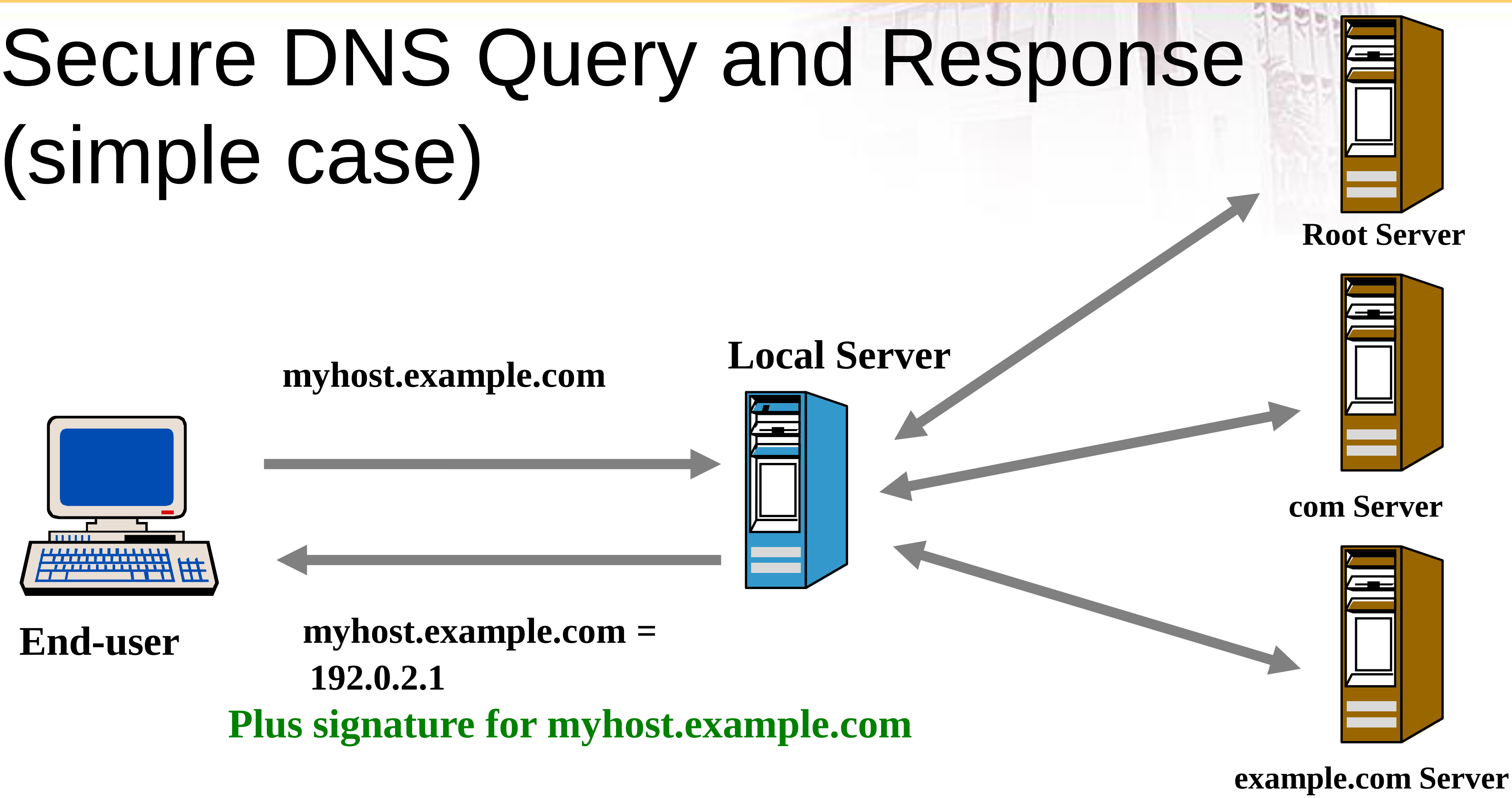
Server Protection

DATA Protection

The Problem

- DNS data is too readily changed, removed or replaced between the “server” and the “client”.
- This can happen in multiple places in the DNS architecture
  - Some places are more vulnerable than others
  - Vulnerabilities in DNS software make attacks easier (and software will never stop being at risk)

Secure DNS Query and Response (simple case)



Root Server

com Server

example.com Server

Local Server

myhost.example.com

End-user

myhost.example.com =
192.0.2.1

Plus signature for myhost.example.com

Attacker can not forge this answer without the associated private keys.

How Does DNSSEC Extend DNS?

- DNSSEC adds four new record types:
  - DNSKEY - carries public key
  - RRSIG - carries signature of DNS information
  - DS - carries a signed hash of key
  - NSEC (NextSECure) - signs gaps to assure non-existence
- Working on one more, NSEC3
  - “DNSSEC Hashed Authenticated Denial of Existence”. This would provide privacy enhancement.