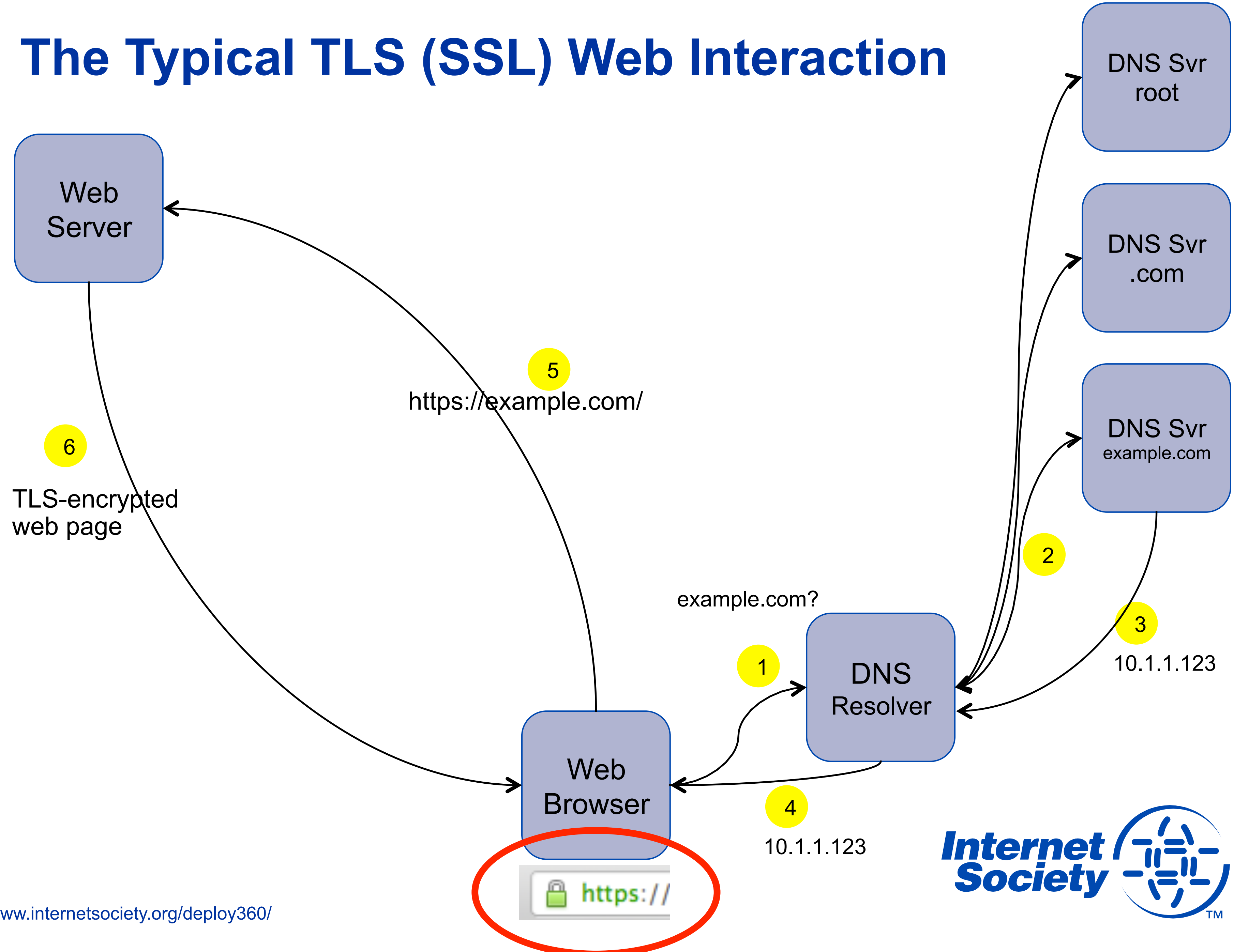
Introduction to the DANE Protocol And Updates From IETF 88

Dan York, Senior Content Strategist
Internet Society

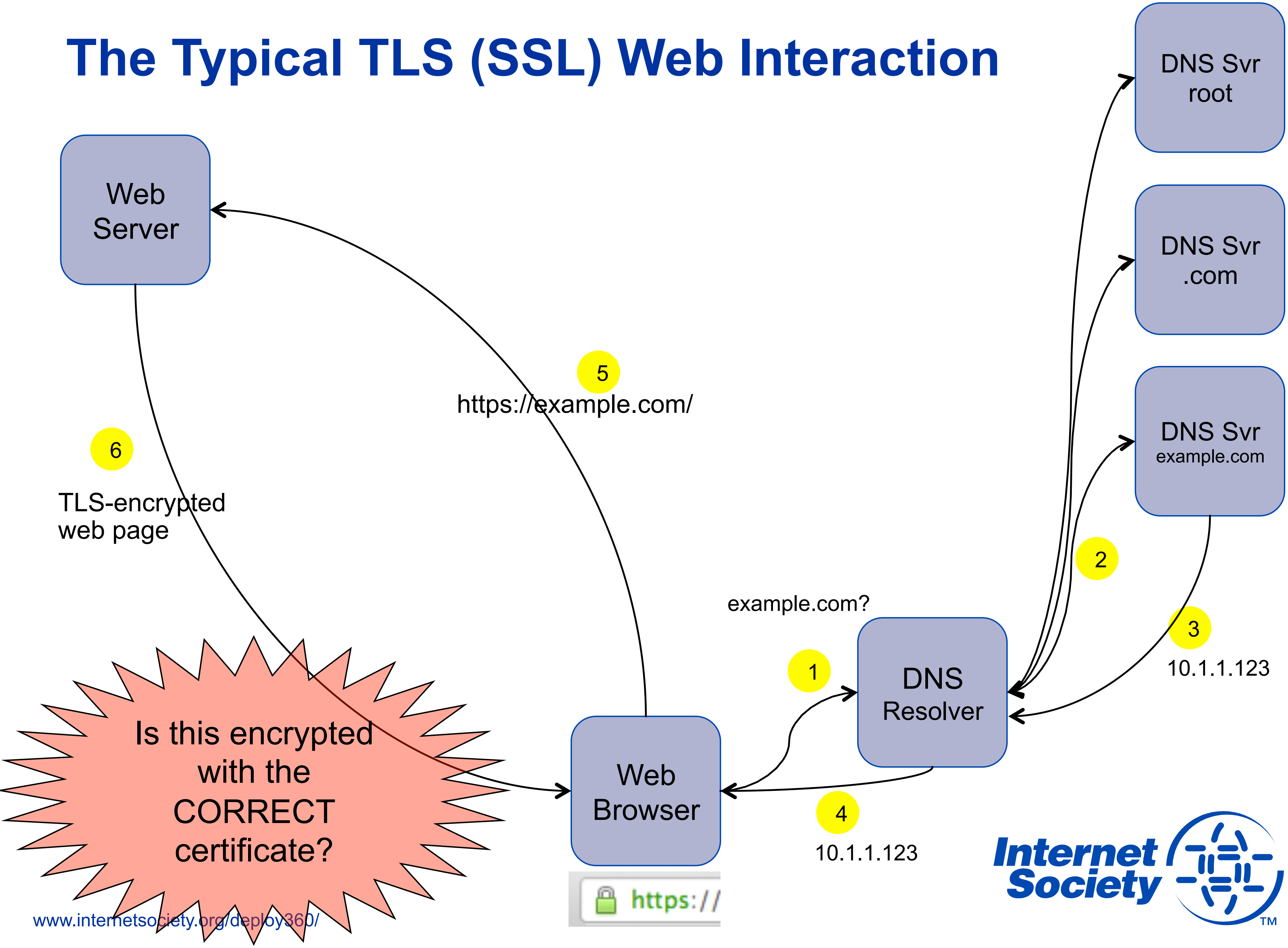
ICANN 48, Buenos Aires, Argentina
November 20, 2013

A Quick Overview of DANE

The Typical TLS (SSL) Web Interaction



The Typical TLS (SSL) Web Interaction



Web Server

DNS Svr root

DNS Svr .com

DNS Svr example.com

5 https://example.com/

6 TLS-encrypted web page

2

example.com?

3 10.1.1.123

1

DNS Resolver

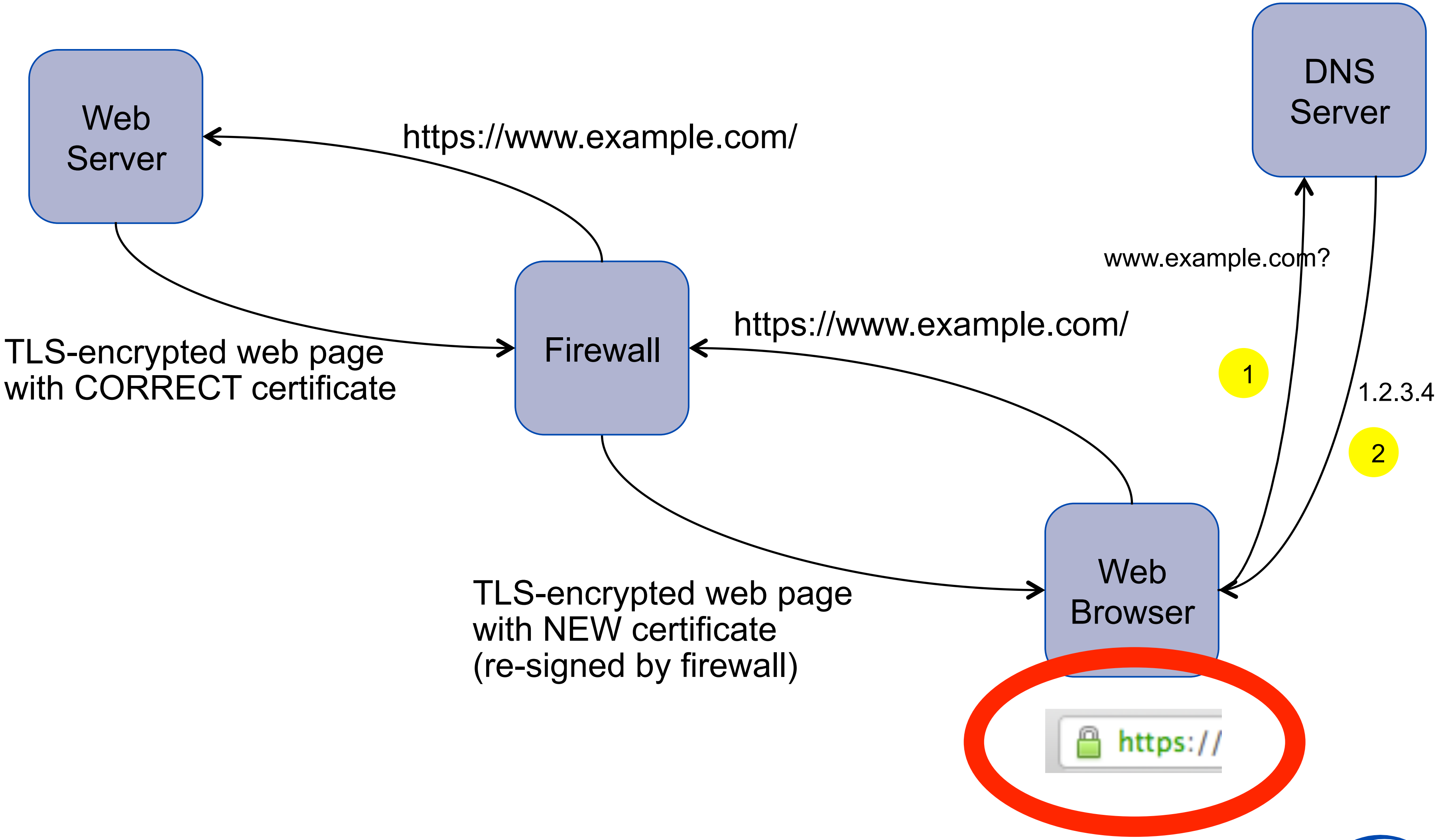
Web Browser

https://

4 10.1.1.123

Is this encrypted with the CORRECT certificate?

Problems?



Web Server

https://www.example.com/

Firewall

TLS-encrypted web page with CORRECT certificate

DNS Server

www.example.com?

https://www.example.com/

1

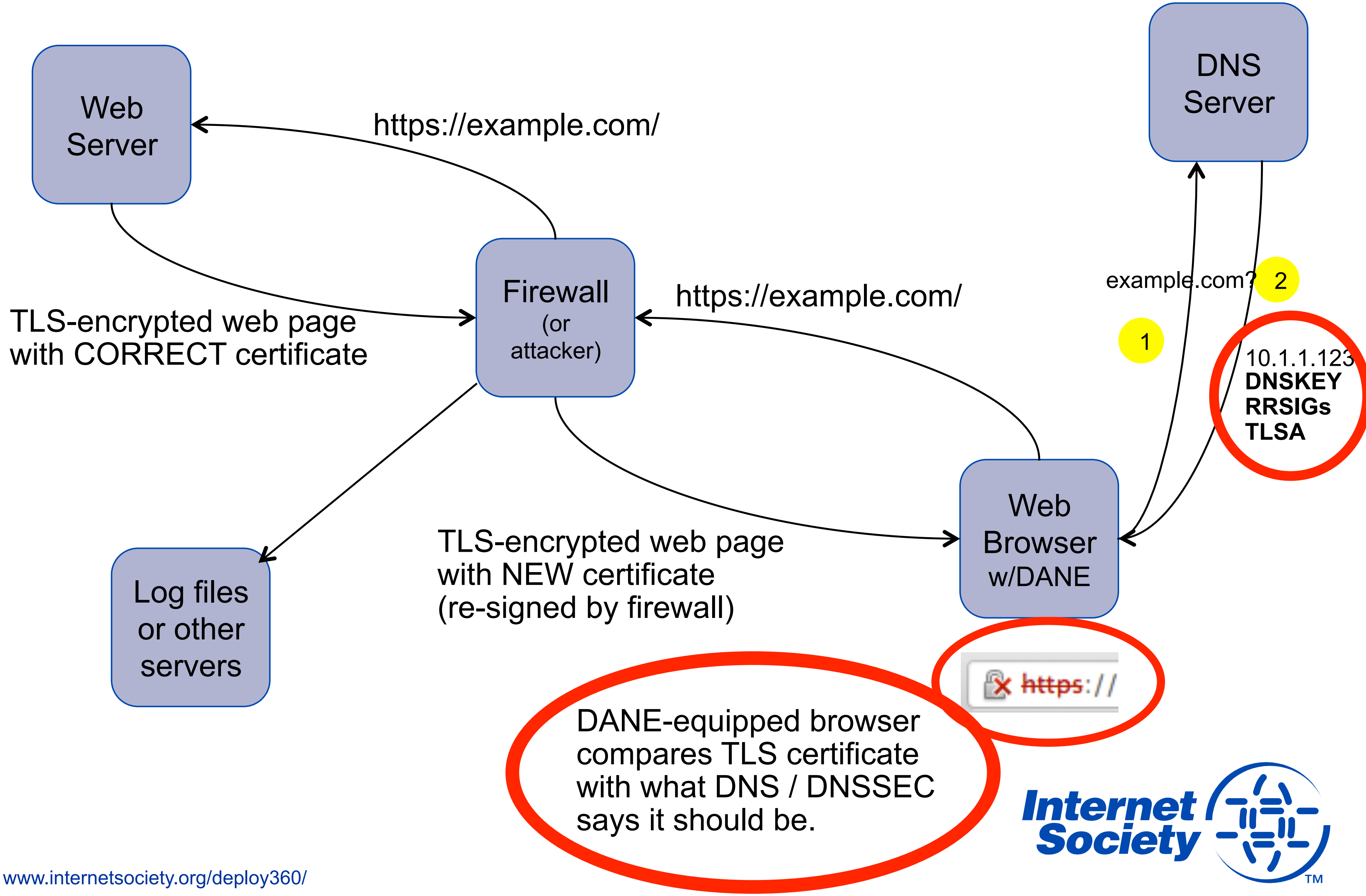
1.2.3.4

2

Web Browser

TLS-encrypted web page with NEW certificate (re-signed by firewall)

DANE



Web Server

https://example.com/

TLS-encrypted web page
with CORRECT certificate

Firewall
(or
attacker)

Log files
or other
servers

https://example.com/

DNS
Server

example.com?

1

2

10.1.1.123
DNSKEY
RRSIGs
TLSA

Web
Browser
w/DANE

TLS-encrypted web page
with NEW certificate
(re-signed by firewall)

~~https~~://

DANE-equipped browser
compares TLS certificate
with what DNS / DNSSEC
says it should be.

www.internetsociety.org/deploy360/

DNS-Based Authentication of Named Entities (DANE)

- Q: How do you know if the TLS (SSL) certificate is the correct one the site wants you to use?

- A: Store the certificate (or fingerprint) in DNS (new TLSA record) and sign them with DNSSEC.

A browser that understand DNSSEC and DANE will then know when the required certificate is NOT being used.

Certificate stored in DNS is controlled by the domain name holder. It could be a certificate signed by a CA – or a self-signed certificate.

The DANE Protocol

- **DANE defined in RFC 6698**
  - https://tools.ietf.org/html/rfc6698
- **Contains either a certificate or the public key of a certificate**
- **Four modes of certificate usage:**
  - 0 – "CA constraint" – limits which CA can be used for certificates
  - 1 – "service certificate constraint" – specifies exact CA-signed certificate
  - 2 – "trust anchor assertion" – allows use of a new trust anchor (such as a CA not included in the browser list)
  - 3 – "domain-issued certificate" – use of self-signed certificate

DANE – Not Just For The Web

- DANE defines protocol for storing TLS certificates in DNS
- Securing Web transactions is the obvious use case
- Other uses also possible:
  - Email via S/MIME
  - VoIP
  - Jabber/XMPP
  - PGP
  - ?
- DANE defined in RFC 6698

DANE Resources

DANE and email:

- **http://tools.ietf.org/html/draft-ietf-dane-smtp**
- **http://tools.ietf.org/html/draft-ietf-dane-smime**

DANE Operational Guidance:

- **http://tools.ietf.org/id/draft-dukhovni-dane-ops-01.txt**

DANE and SIP (VoIP):

- **http://tools.ietf.org/id/draft-johansson-dane-sip-00.txt**

Other uses:

- **http://tools.ietf.org/id/draft-wouters-dane-openpgp-00.txt**
- **http://tools.ietf.org/id/draft-wouters-dane-otrfp-00.txt**

DANE Resources

DANE Overview and Resources:

- **http://www.internetsociety.org/deploy360/resources/dane/**

IETF Journal article explaining DANE:

- **http://bit.ly/dane-dnssec**

RFC 6394 - DANE Use Cases:

- **http://tools.ietf.org/html/rfc6394**

RFC 6698 – DANE Protocol:

- **http://tools.ietf.org/html/rfc6698**

Increased Number Of DNSSEC Tools

Lists of tools:

http://www.internetsociety.org/deploy360/dnssec/tools/

http://www.internetsociety.org/deploy360/blog/tag/tools/

DNSSEC Tools Project

http://www.dnssec-tools.org/

Helping Accelerate DNSSEC Deployment

Public mailing list, “dnssec-coord”, available and open to all:

https://elists.isoc.org/mailman/listinfo/dnssec-coord

Focus is on better *coordinating* promotion / advocacy / marketing activities related to DNSSEC deployment.

Monthly conference calls and informal meetings at ICANN and IETF events.

An Update On DNS At IETF 88

IETF 88 – November 3-8, Vancouver, BC

Photo courtesy of Brian Campbell

IETF 88 last week in Vancouver

- www.ietf.org/meeting/88/

~1200 participants from 54 countries

Focus on pervasive monitoring and possible security improvements

Our posts about IETF88 at:

- http://www.internetsociety.org/deploy360/blog/tag/ietf88/

DNS/DNSSEC Activities

- **DNS Operations (DNSOP) WG**
  - Focus on automation of DNSSEC including communication between zones
- **Side meeting focused on the DANE protocol**
  - Lunch-time meeting brought together 25-30 people
- **DNS-SD Extensions (DNSSD) WG**
  - Focus on using extending DNS for service discovery beyond a local network using Multicast DNS (RFC 6762) and DNS-Based Service Discovery (RFC 6763)

DNSOP Working Group

- **DNS Operations (DNSOP) WG – Nov 5, 2013**
  - https://tools.ietf.org/wg/dnsop/agenda
- **Automating transmission of updated key material from DNS Operator to Registry:**
  - CDS/CDNSKEY Records
    - https://tools.ietf.org/agenda/88/slides/slides-88-dnsop-1.pdf
  - DNS UPDATE
    - https://tools.ietf.org/html/draft-andrews-dnsop-update-parent-zones
- **DS Query Increases**
  - https://tools.ietf.org/html/draft-fujiwara-dnsop-ds-query-increase
- **Increasing Efficiency of DNSSEC Communication**
  - https://tools.ietf.org/agenda/88/slides/slides-88-dnsop-6.pdf

DNSOP Working Group, continued

- **More documents and slides on:**
  - https://tools.ietf.org/wg/dnsop/agenda
- **DNSSEC Roadblock Avoidance**
  - https://tools.ietf.org/agenda/88/slides/slides-88-dnsop-11.pdf
- **Other DNSOP documents:**
  - https://tools.ietf.org/wg/dnsop/

DANE Side Meeting

- **Lunch-time meeting focused on the DANE protocol**
- **Key points:**
  - Need to get more TLSA records deployed.
  - Need to improve the ease of generating TLSA records.
  - Exploration of types of DANE usage other than web browsers
- **DANE terminology:**
  - https://tools.ietf.org/html/draft-ogud-dane-vocabulary
- **DANE test tool from NIST:**
  - https://www.had-pilot.com/dane/danelaw.html

IETF 88 – Focus On Strengthening The Internet

Major focus on hardening the Internet against pervasive monitoring and large-scale surveillance

IETF 88 Technical Plenary focused on security:

- http://www.ietf.org/live/ietf88/

Security focus throughout working groups

IETF Chair blog post summarizing the activity:

- http://www.ietf.org/blog/2013/11/we-will-strengthen-the-internet/

IETF 88 – More Information

Photo courtesy of Brian Campbell

IETF 88 last week in Vancouver

- http://www.ietf.org/meeting/88/

Meeting Materials

- https://datatracker.ietf.org/meeting/88/materials.html

Our posts about IETF88 at:

- http://www.internetsociety.org/deploy360/blog/tag/ietf88/

IETF 88 Technical Plenary

- http://www.ietf.org/live/ietf88/

Help The IETF Create Better Standards

To Learn More:

- **http://www.ietf.org/newcomers.html**

Particularly:

IPv6 Operations (V6OPS)

DNS Operations (DNSOP)

You can:

- Join the mailing lists
- Read the drafts and provide comments

Dan York

Senior Content Strategist
Internet Society

york@isoc.org

http://www.internetsociety.org/deploy360/

Thank You!

Internet Society ™