Introduction to Computer Networks
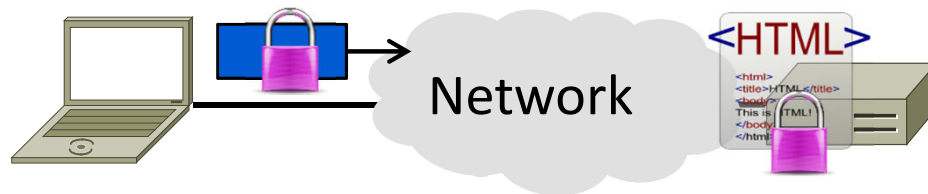
Web Security (§8.9.3, §8.5)

David Wetherall (djw@uw.edu)

Professor of Computer Science & Engineering

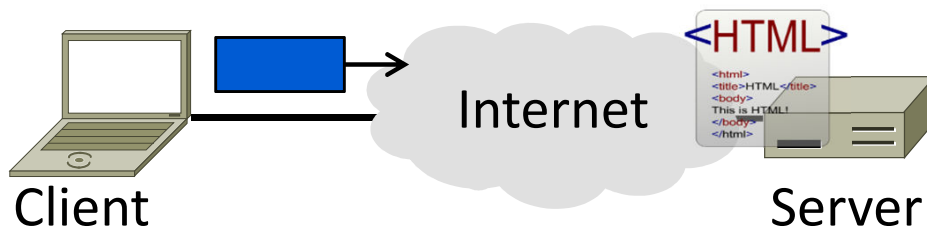UNIVERSITY *of* WASHINGTON

Topic

- Securing the web
 - Focus on SSL/TLS for HTTPS
  - Including certificates

Goal and Threat Model

- Much can go wrong on the web!
  - Clients encounter malicious content
  - Web servers are target of break-ins
  - Fake content/servers trick users
 - Data sent over network is stolen …

Goal and Threat Model (2)

- Goal of HTTPS is to secure HTTP
- We focus on network threats:
  1. Eavesdropping client/server traffic
  2. Tampering with client/server traffic
  3. Impersonating web servers

Network

Client   Server
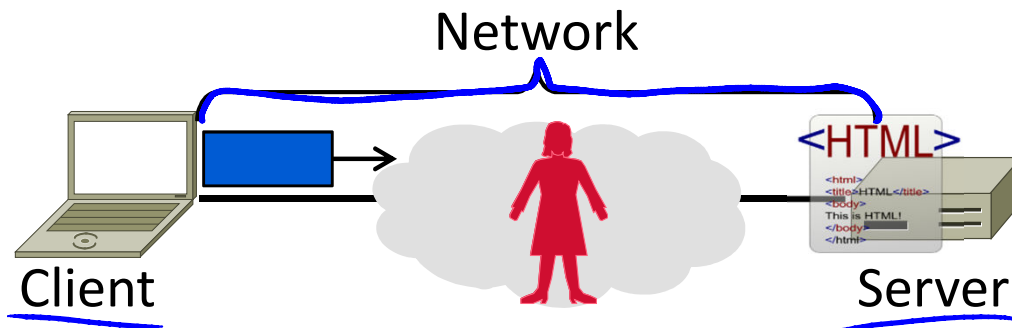
HTTPS Context

- HTTPS (HTTP Secure) is an add-on
  - Means HTTP over SSL/TLS
  - SSL (Secure Sockets Layer) precedes TLS (Transport Layer Security)

HTTPS
| HTTP |
| SSL/TLS | ← Insert
| TCP |
| IP |
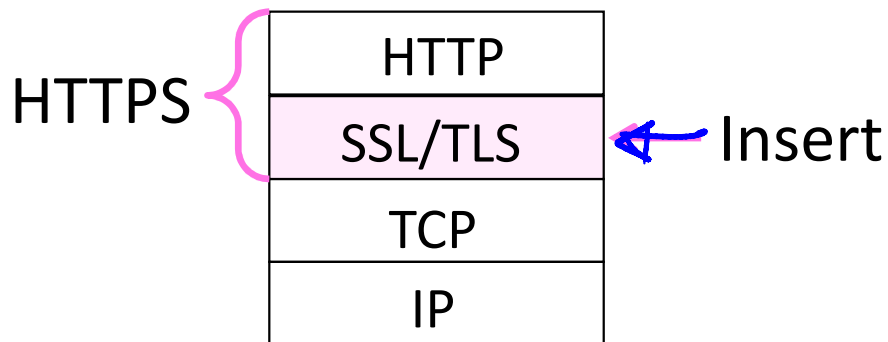
HTTPS Context (2)

- SSL came out of Netscape
  - SSL2 (flawed) made public in '95
  - SSL3 fixed flaws in '96
- TLS is the open standard
  - TLS 1.0 in '99, 1.1 in '06, 1.2 in '08

- Motivated by secure web commerce
  - Slow adoption, now widespread use
  - Can be used by any app, not just HTTP

SSL Operation

- Protocol provides:
    1. Verification of identity of server (and optionally client)
    2. Message exchange between the two with confidentiality, integrity, authenticity and freshness

- Consists of authentication phase (that sets up encryption) followed by data transfer phase

SSL/TLS Authentication

- Must allow clients to securely connect to servers not used before
  - Client must authenticate server 🔒
  - Server typically doesn't identify client

- Uses public key authentication
  - But how does client get server's key?
  - With certificates »

Certificates

- A certificate binds public key to an identity, e.g., domain
  - Distributes public keys when signed by a party you trust
  - Commonly in a format called X.509

I hereby certify that the public key
19836A8B03030CF83737E3837837FC3s87092827262643FFA82710382828282A
belongs to
Robert John Smith
12345 University Avenue
Berkeley, CA 94702
Birthday: July 4, 1958
Email: bob@superdupernet.com

Signed by CA
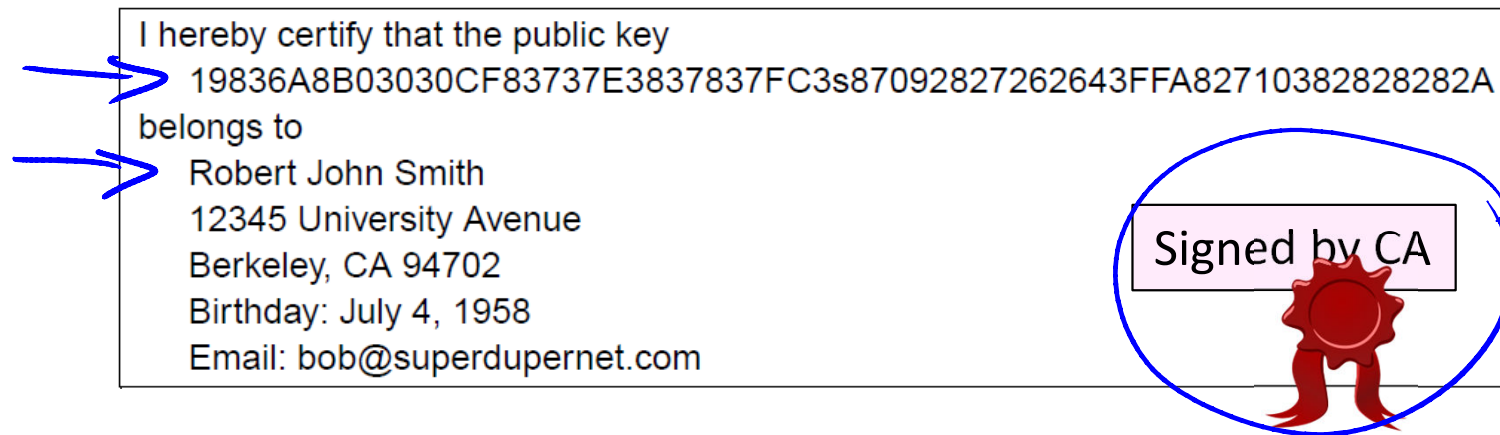
PKI (Public Key Infrastructure)

- Adds hierarchy to certificates to let many parties issue
  - Issuing parties are called CAs (Certificate Authorities)
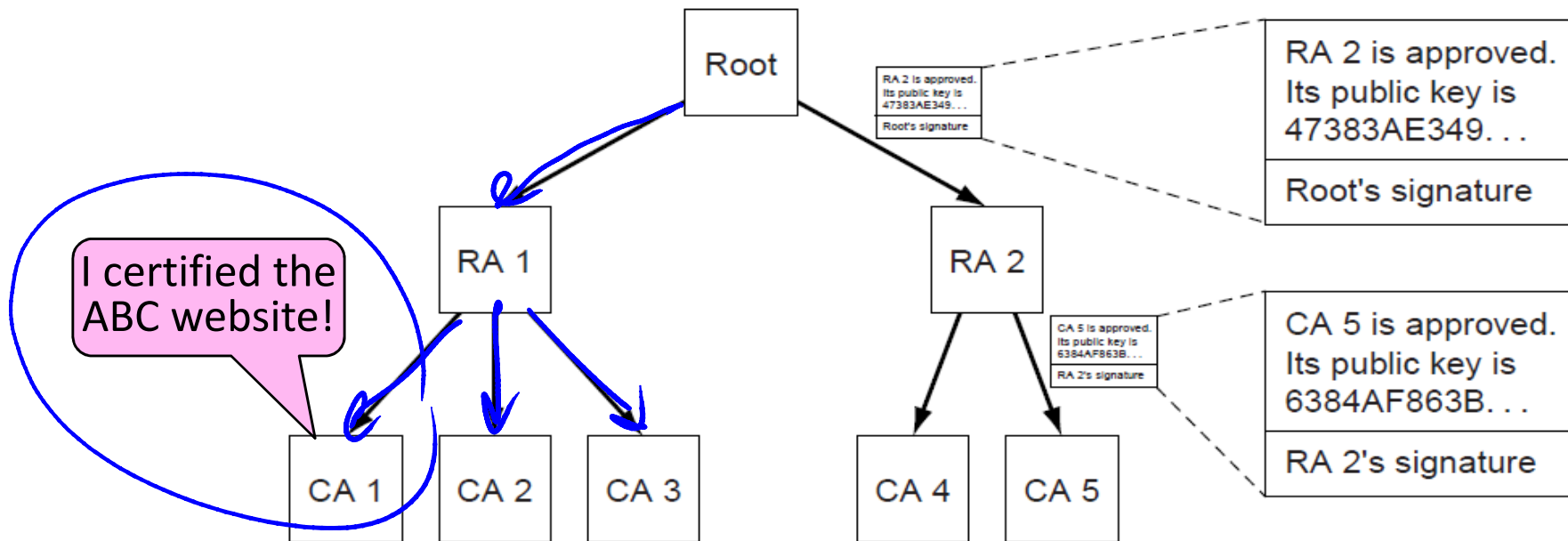
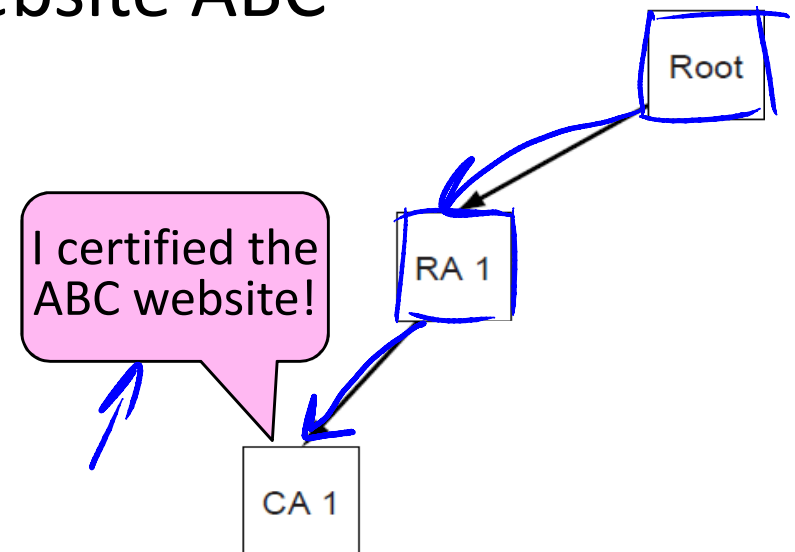# PKI (2)

- Need public key of PKI root and trust in servers on path to verify a public key of website ABC
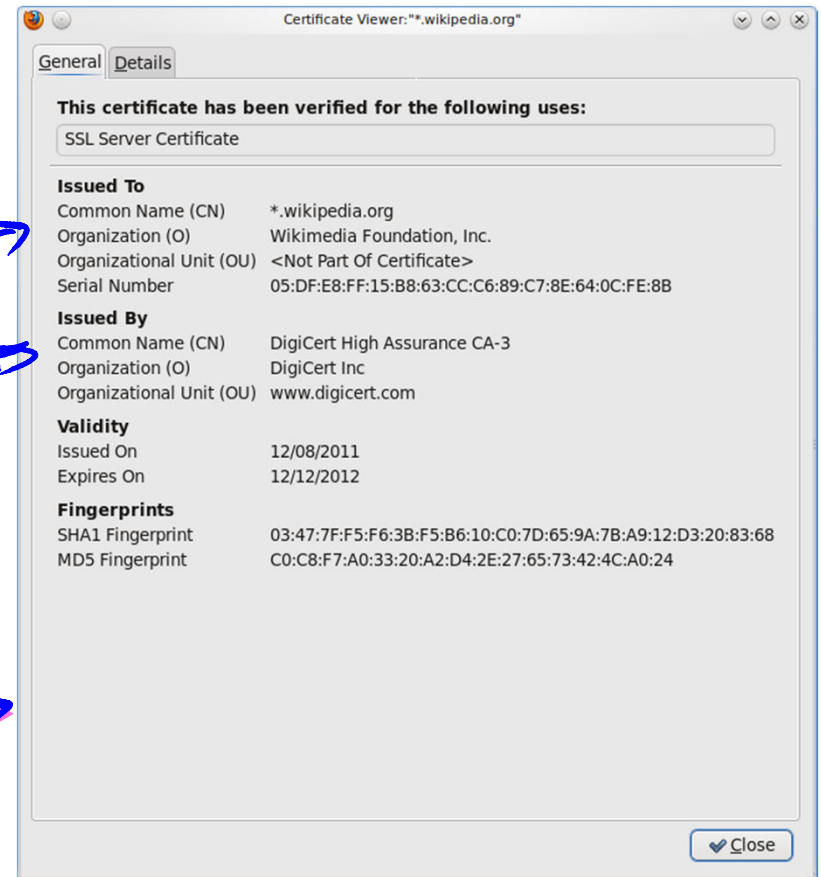
  Browser has Root's public key

  {RA1's key is X} signed Root

  {CA1's key is Y} signed RA1 (X)

  {ABC's key Z} signed CA1 (Y)

I certified the ABC website!

Root

RA 1

CA 1

PKI (3)

- Browser/OS has public keys of the trusted roots of PKI
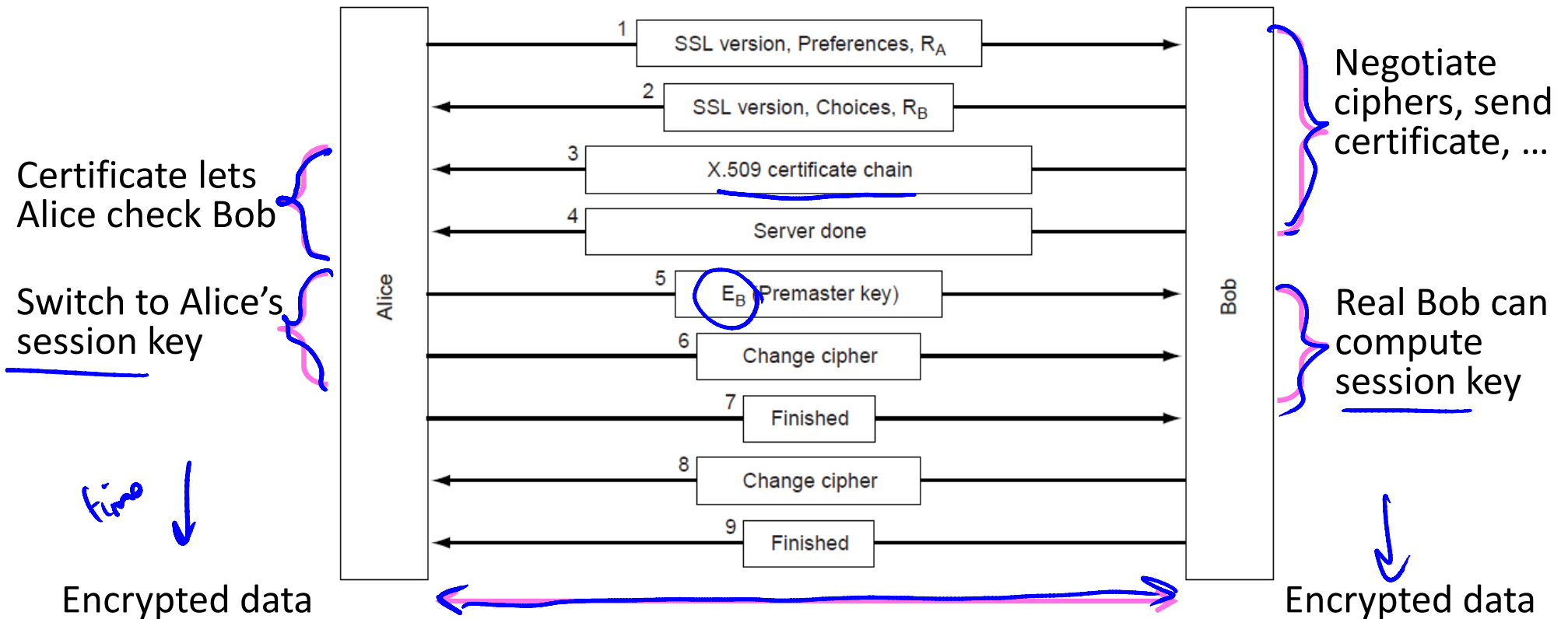   - >100 root certificates!
    - That's a problem …
    - Inspect your web browser

Certificate for wikipedia.org issued by DigiCert

Certificate Viewer: "*.wikipedia.org"

General | Details

This certificate has been verified for the following uses:

SSL Server Certificate

Issued To
Common Name (CN)   *.wikipedia.org
Organization (O)   Wikimedia Foundation, Inc.
Organizational Unit (OU)   <Not Part Of Certificate>
Serial Number   05:DF:E8:FF:15:B8:63:CC:C6:89:C7:8E:64:0C:FE:8B

Issued By
Common Name (CN)   DigiCert High Assurance CA-3
Organization (O)   DigiCert Inc
Organizational Unit (OU)   www.digicert.com

Validity
Issued On   12/08/2011
Expires On   12/12/2012

Fingerprints
SHA1 Fingerprint   03:47:7F:F5:F6:3B:F5:B6:10:C0:7D:65:9A:7B:A9:12:D3:20:83:68
MD5 Fingerprint   C0:C8:F7:A0:33:20:A2:D4:2E:27:65:73:42:4C:A0:24

Close

PKI (4)

- Real-world complication:
  - Public keys may be compromised
  - Certificates must then be revoked

- PKI includes a CRL (Certificate Revocation List)
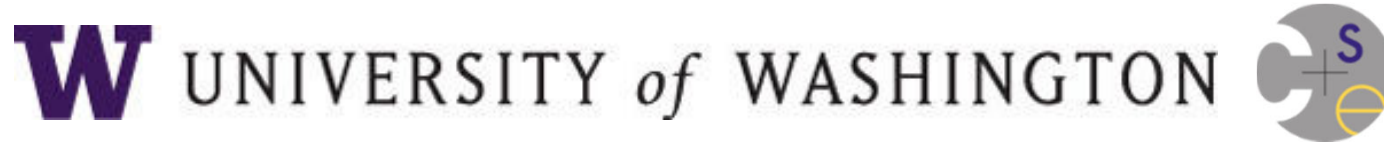 - Browsers use to weed out bad keys

SSL3 Authentication (2)

Negotiate ciphers, send certificate, …

Certificate lets Alice check Bob

Switch to Alice's session key

Real Bob can compute session key

time

Encrypted data

Encrypted data

1	SSL version, Preferences, R_A	
2	SSL version, Choices, R_B	
3	X.509 certificate chain	
4	Server done	
5	E_B (Premaster key)	
6	Change cipher	
7	Finished	
8	Change cipher	
9	Finished	

Takeaways

- SSL/TLS is a secure transport
    - For HTTPS and more, with the usual confidentiality, integrity / authenticity
    - Very widely used today

- Client authenticates web server
    - Done with a PKI and certificates
    - Major area of complexity and risk

END

UNIVERSITY *of* WASHINGTON