

Computer Networks

Web Security (§8.9.3, §8.5)



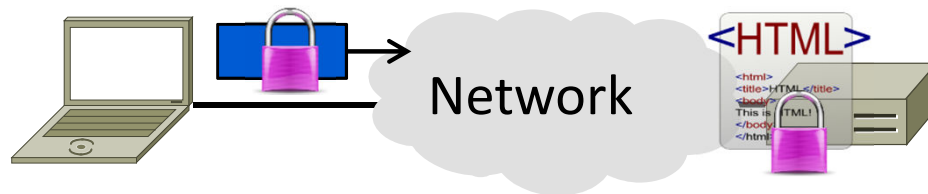
David Wetherall (djw@uw.edu)

Professor of Computer Science & Engineering

UNIVERSITY *of* WASHINGTON

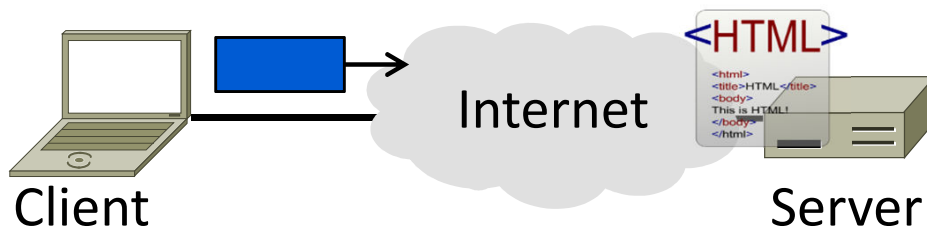
Topic

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



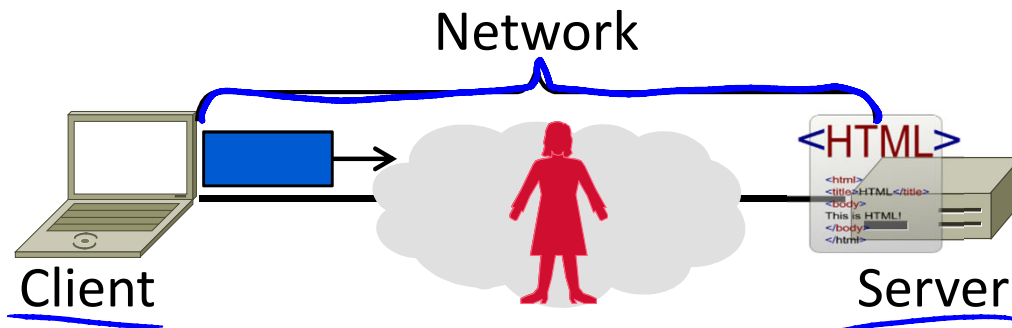
Goal and Threat Model

- 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 ...



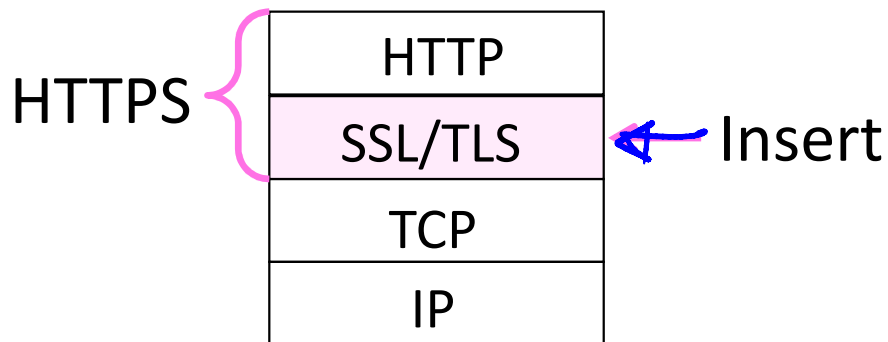
Goal and Threat Model (2)

- 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





HTTPS Context

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




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

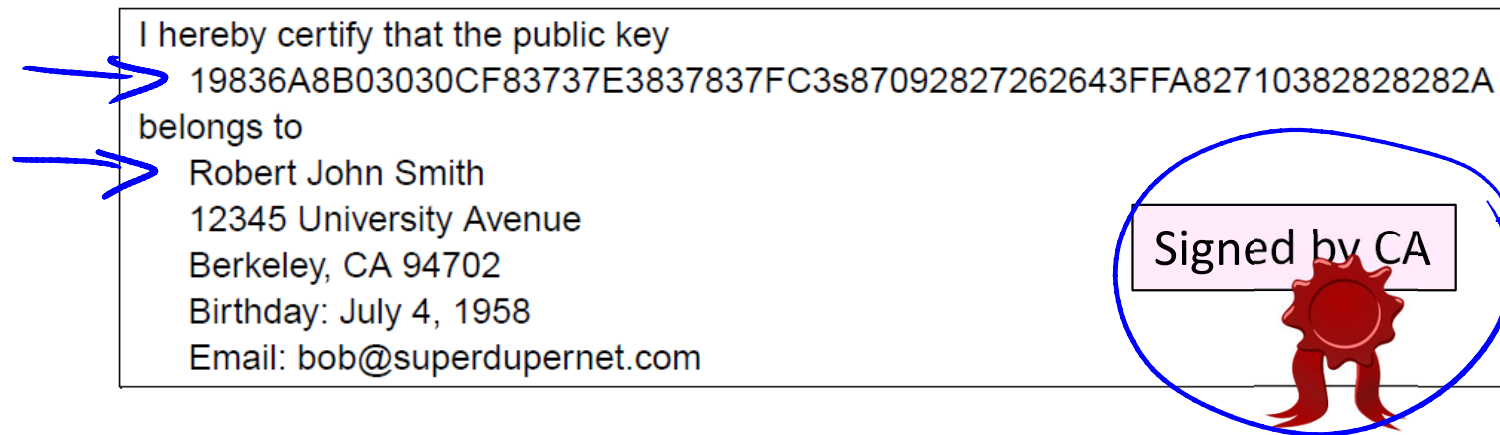
- Protocol provides:
 - 1. Verification of identity of server (and optionally client)
 - 2. Message exchange between the two with confidentiality, integrity, authenticity and freshness
- Consists of authentication phase (that sets up encryption) followed by data transfer phase

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 »

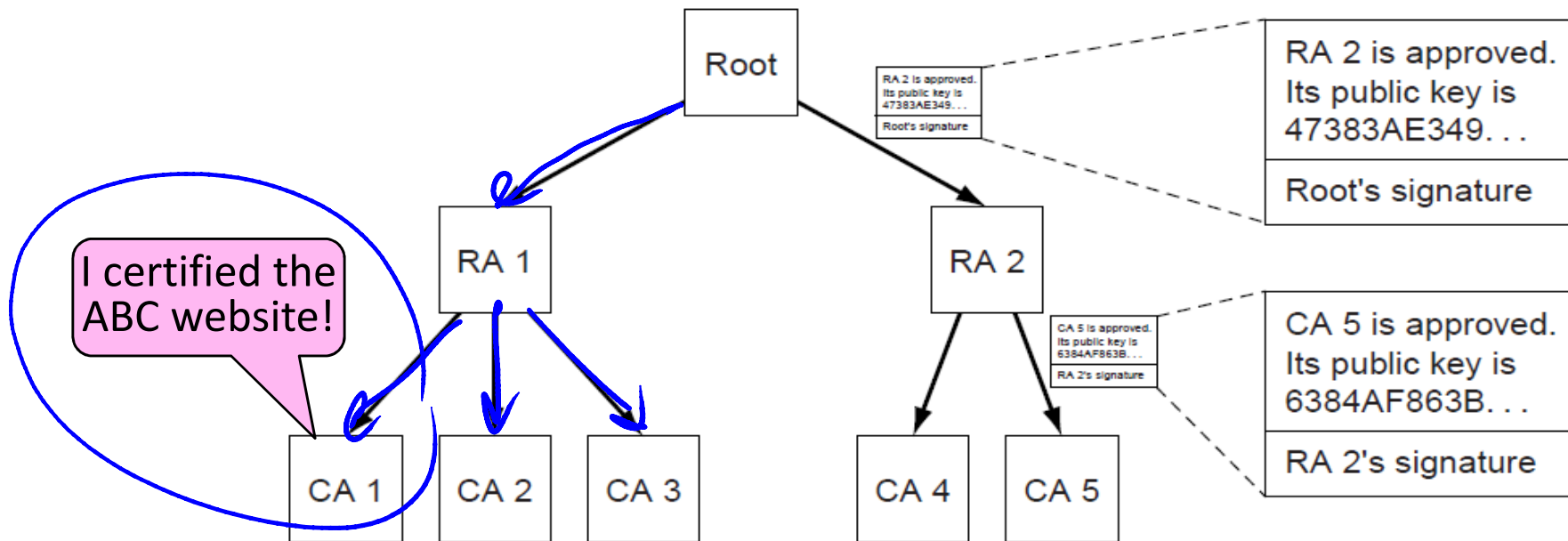
Certificates

- 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



PKI (Public Key Infrastructure)

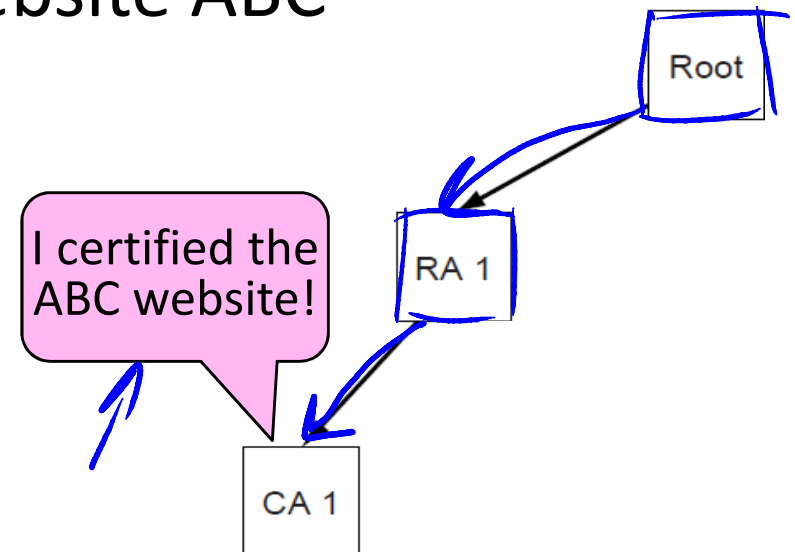
- Adds hierarchy to certificates to let many parties issue
 - Issuing parties are called CAs (Certificate Authorities)



PKI (2)

- Need public key of PKI root and trust in servers on path to verify a public key of website ABC

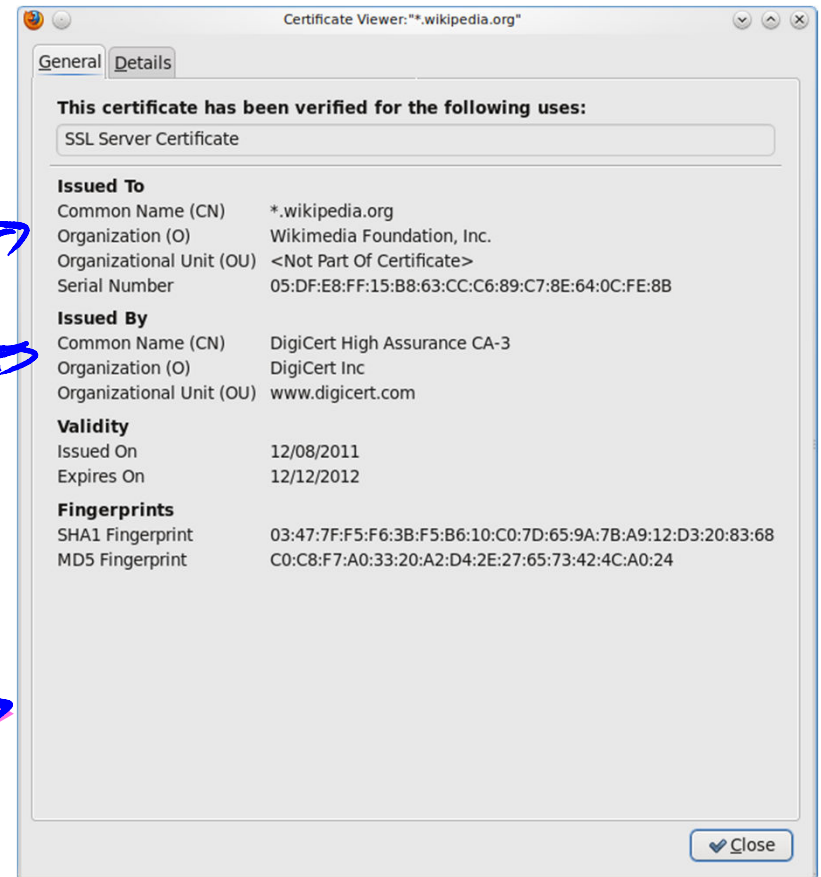
- Browser has Root's public key
- {RA1's key is X} signed Root
- {CA1's key is Y} signed RA1(X)
- {ABC's key Z} signed CA1 (Y)



PKI (3)

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

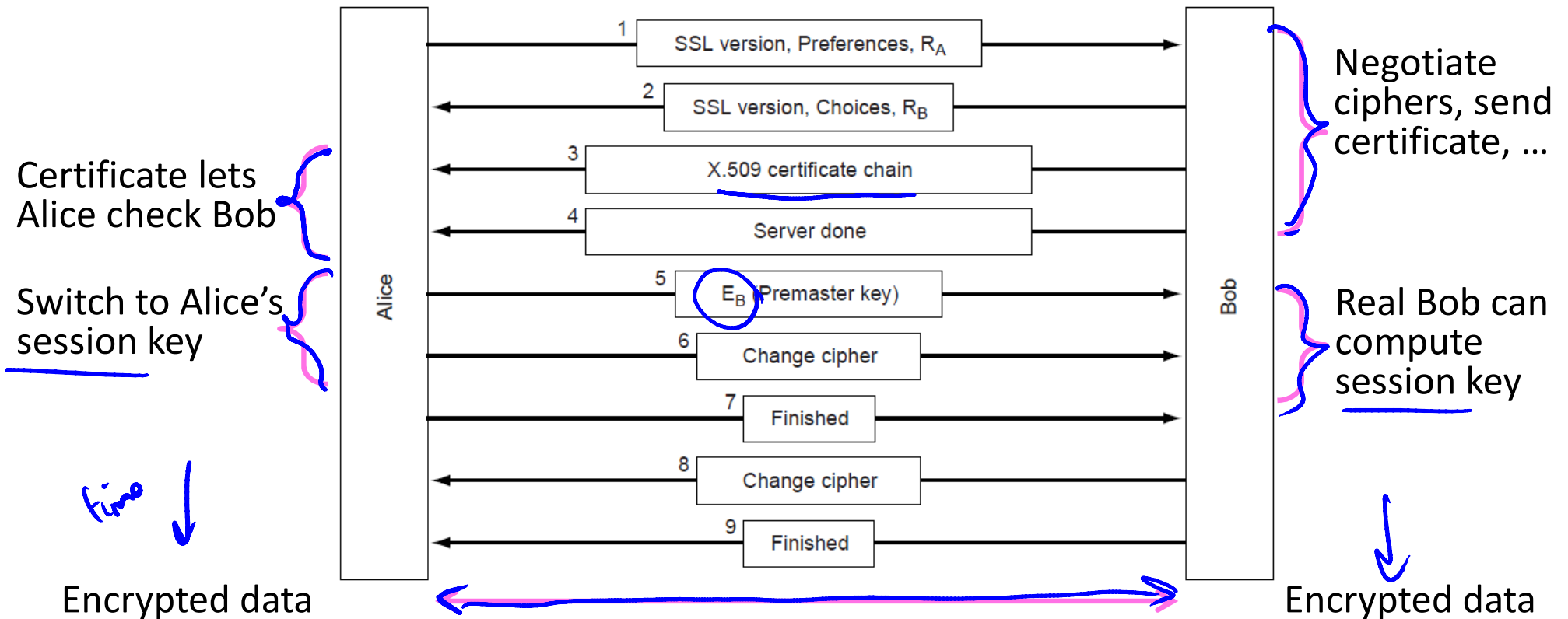
Certificate for wikipedia.org
issued by DigiCert







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)



Takeaways

-  SSL/TLS is a secure transport
 - For HTTPS and more, with the usual confidentiality, integrity / authenticity
 - Very widely used today CN5E slides #8-40
-  Client authenticates web server
 -  Done with a PKI and certificates
 -  Major area of complexity and risk

END

© 2013 D. Wetherall

Slide material from: TANENBAUM, ANDREW S.; WETHERALL, DAVID J., COMPUTER NETWORKS, 5th Edition, © 2011.
Electronically reproduced by permission of Pearson Education, Inc., Upper Saddle River, New Jersey