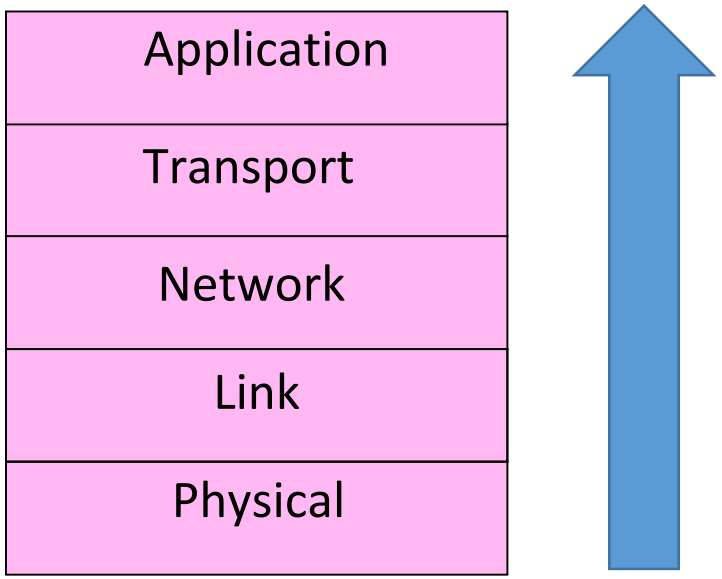
Network Security

Where we are in the Course

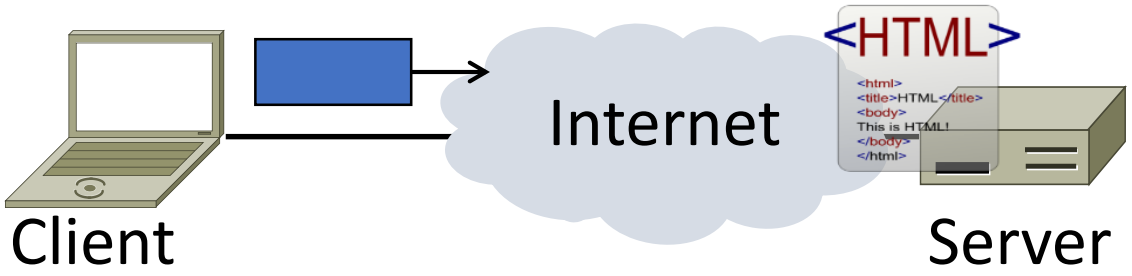
- Security crosses all layers



Web Security

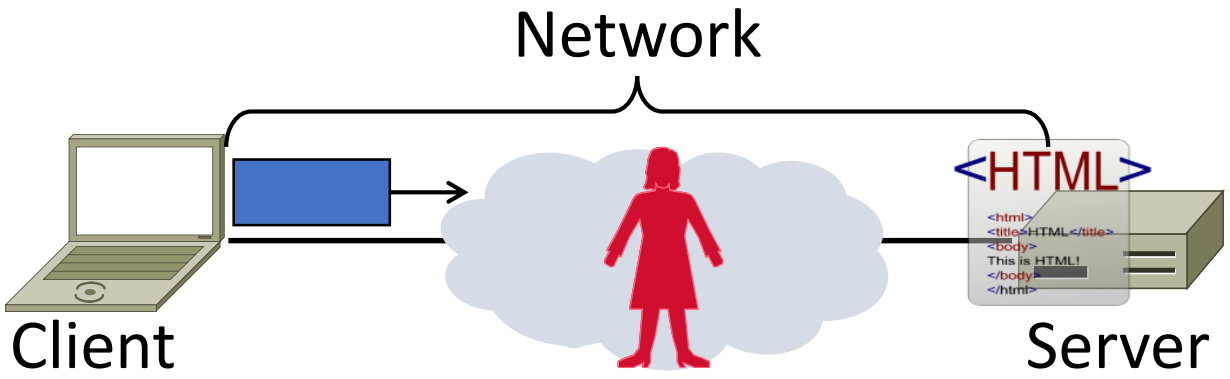
Goal and Threat Model

- 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 …



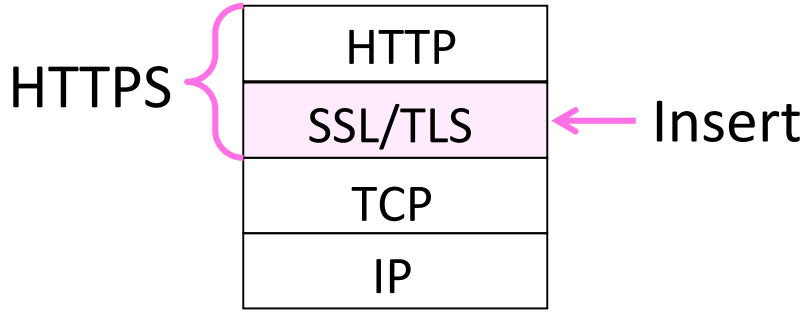
Goal and Threat Model (2)

- 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

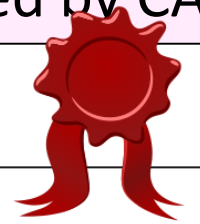
- Must allow clients to securely connect to servers not used before
  - Client must authenticate server
  - Server typically doesn't identify client
- Uses public key authentication
  - But how does client get server's key?
  - With certificates »

Certificates

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

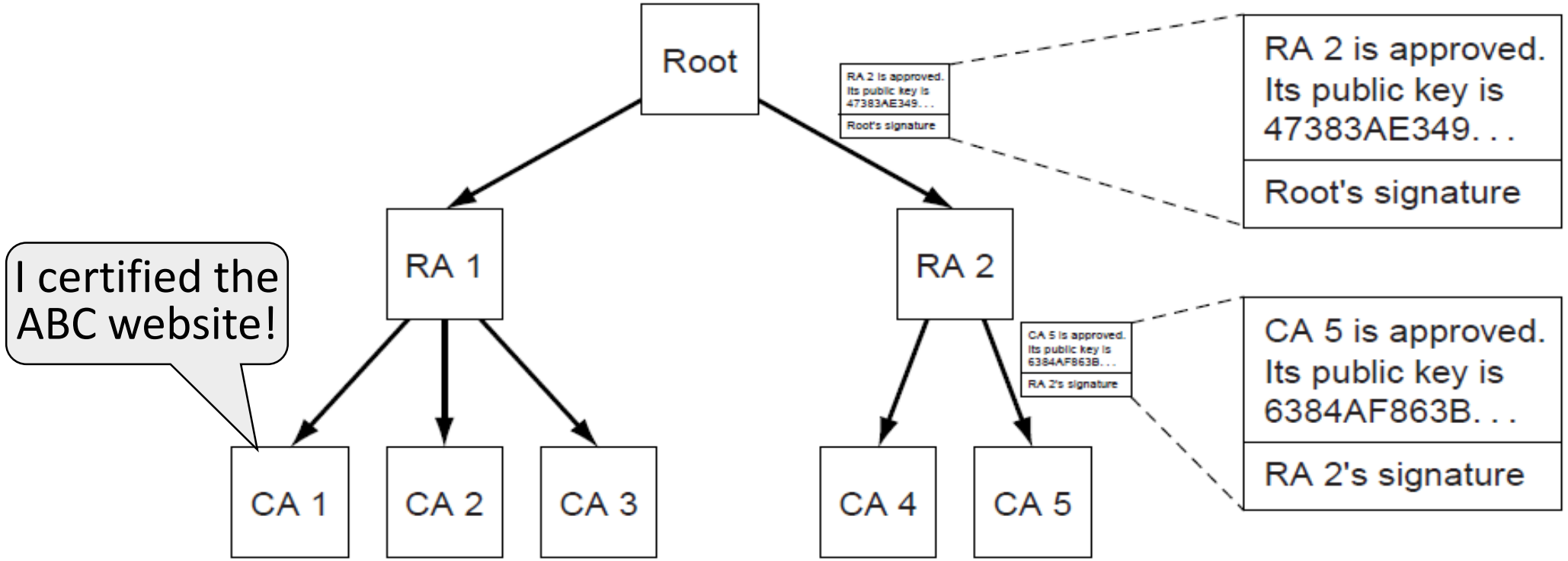
I hereby certify that the public key
19836A8B03030CF83737E3837837FC3s87092827262643FFA82710382828282A
belongs to
Robert John Smith
12345 University Avenue
Berkeley, CA 94702
Birthday: July 4, 1958
Email: bob@superdupernet.com

Signed by CA



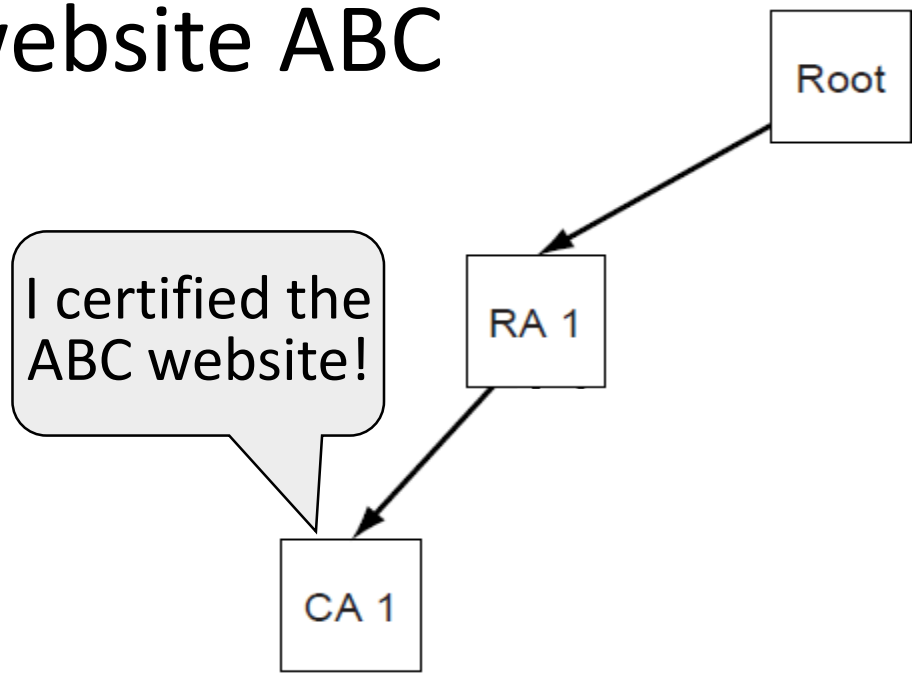
PKI (Public Key Infrastructure)

- Adds hierarchy to certificates to let 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
  - {ABC's key Z} signed CA1



PKI (3)

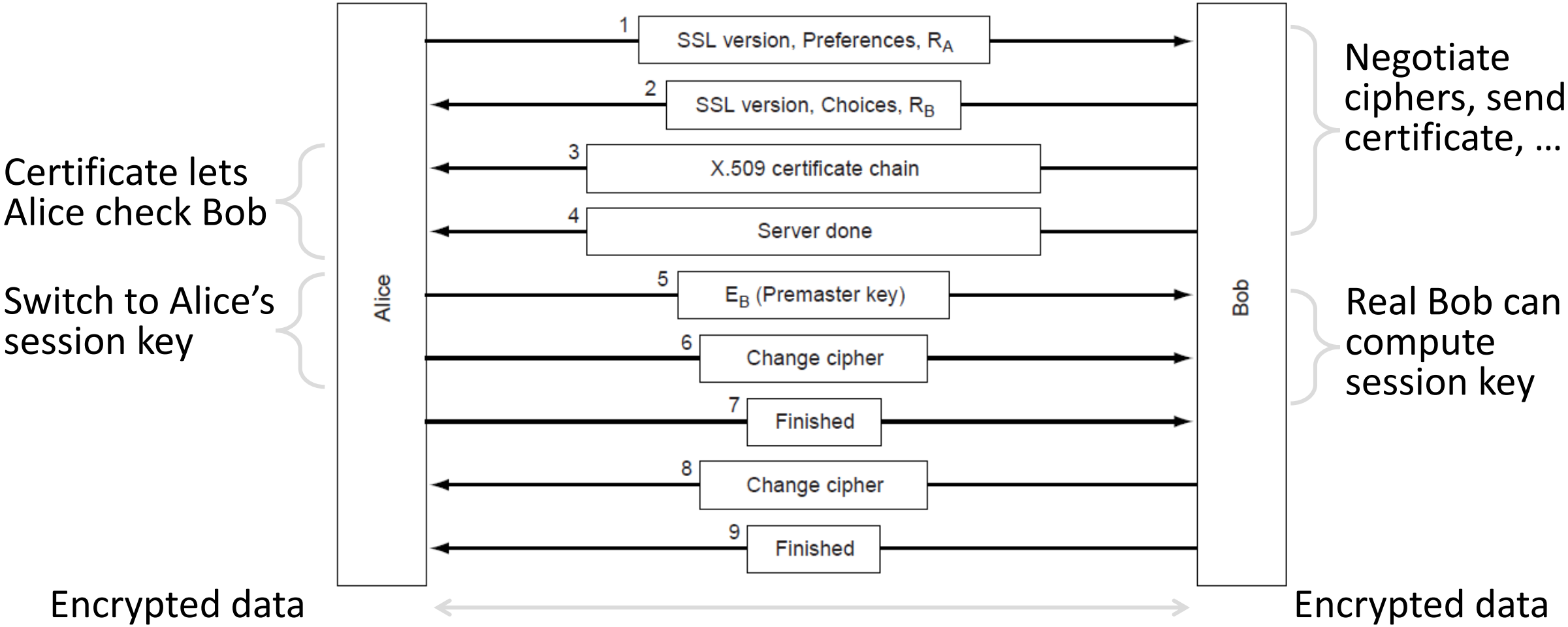
- Browser/OS has public keys of the trusted roots of PKI
  - >100 root certificates!
  - That's a problem …
  - Inspect your web browser

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)



“Metadata”

- What can attacker still learn from an HTTPS connection?

Tor

- “The Onion Router”
- Basic idea:
  1. Generate circuit of routers that you know will send packet
  2. Encrypt the packet in layers for each router in circuit
  3. Send the packet
  4. Each router receives, decrypts their layer, and forwards based on new info
  5. Routers maintain state about circuit to route stuff back to sender
     - But again, only know the next hop

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
- “Metadata” leaks
  - Use other tools (Tor) if you want to hide that