SSL / TLS

Slides by Prof. Jonathan Katz.
Lightly edited by me.

SSL/TLS

- How can you securely send your credit card number to Amazon?

- SSL/TLS
  - Secure Socket Layer (Netscape, mid-’90s)
  - Transport Layer Security
    - TLS 1.0 (1999)
    - TLS 1.2 (2008)
    - TLS 1.3 (2018)
  - Used by every web browser for https connections

SSL/TLS

- Goals
  - Understand (at a high level) a real-world crypto protocol
  - Pull together everything learned in this course
- Not goals
  - Understanding low-level details/implementation
  - Defining or proving security

SSL/TLS

- Two phases
  - Handshake protocol
    - Establish a shared key between two entities
  - Record-layer protocol
    - Use the shared key for secure communication

Handshake protocol

https://bank.com, N_C

pk, cert, N_B

Verify!

pk_{CA}

$c = Enc_{pk}(pmk)$

sk, pk, $cert_{CA \rightarrow Bank}$

~~$mk = H(pmk, N_C, N_B)$~~
$k_C, k'_C, k_S, k'_S = G(mk)$

$Mac_{mk}(transcript)$

$pmk = Dec_{sk}(c)$
~~$mk = H(pmk, N_C, N_B)$~~
$k_C, k'_C, k_S, k'_S = G(mk)$

Verify!

$Mac_{mk}(transcript')$

Verify!

Record-layer protocol

- Parties now share k_C, k'_C, k_S, k'_S
- Client uses k_C, k'_C to encrypt/authenticate all messages it sends
- Server uses k_S, k'_S to encrypt/authenticate all messages it sends
  - Prevents reflection attacks
- Sequence numbers prevent replay attacks