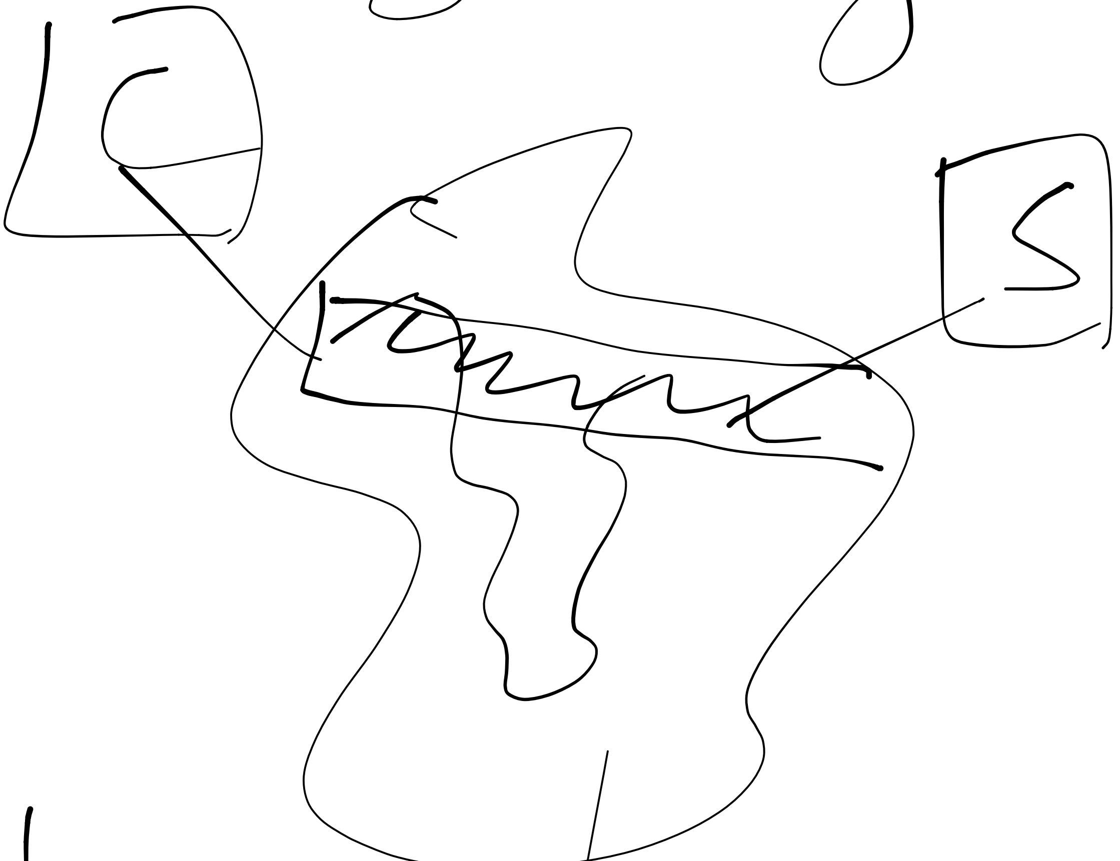
6.858

SSL/TLS

Network Security



Liveness

Secure channel

Authenticity

Confidentiality

Strong foundation

Well understood

Crypto

Encryption → Confidentiality

Signatures → Authenticity

Public key

Symmetric key

Public key

Keygen → (Pk, Sk)

Encrypt(Pk, m) → c

Decrypt(Sk, c) → m

Sign(Sk, m) → sig

Verify(Pk, m, sig) → t / f

RSA, elliptic curve

Symmetric key

Keygen() → k

Encrypt(k, m) → c

Decrypt(k, c) → m

MAC(k, m) → tag

AES

XOR

Secure channel

1 C → S : connect

2 C ← S : PK_S

3 C → S : $E(PK_S, k)$

4. C ↔ S : $E(m, k)$

Forward Secrecy

Sol I: certificates

Certificate Authority

Name	Key
mit.edu	pk

$\{\text{name}, pk\}_{SKA}$

2': C <— S

name, $\underline{Pk}_s$,

$\{$name, Pks$\}_{SKA}$

Authenticating msg

''Transfer $1 to Bob'

C

''Transfer $100 to bob''

Authenticated Encryption

$$C = E(k, m) \| MAC(k, m)$$

Replay : sequence number

Forward secrecy

Short-lived keys for encryption

2'. $C \leftarrow S$: SK_s

Pk_conn, Sign(Pk_s, Pk_conn), certificate

$C \rightarrow S$: E(Pk_conn,

k)

SSL/TLS

Secure channel for the Web

SSL 1.0, 2.0, ~~3.0~~

TLS 1.0, 1.1, 1.2, 1.3

2006 2008

Attacks

2.0: edit client hello msg

3.0: version roll back attack.

marker

3.0: drop change cipher

↓

TLS 1.0 → Heartbleed

Poodle

POST path

Cookie: pw: <val>

\n\r\n\r body

SSL:

$$E(\underbrace{msg}_{16}\underbrace{||mac}_{16}||pad)$$

last byte

contains length of padding

Attack

1) Arrange for full block of padding

2) first byte of cookie is the last byte of block

3) C_i copies into padding

$$C_i[15] \approx \frac{\text{length}}{15}$$

$$D(K, C_i)[15] = \overline{15}$$

$$\underline{M_i \oplus C_{i-1} \oplus C_n[15]} = \underline{15}$$

$$M_i[15] = 15 \oplus$$. ✓ :

Summary

Secure channel

foundation

→ don't design your own protocols

Security problems

not in crypto protocols