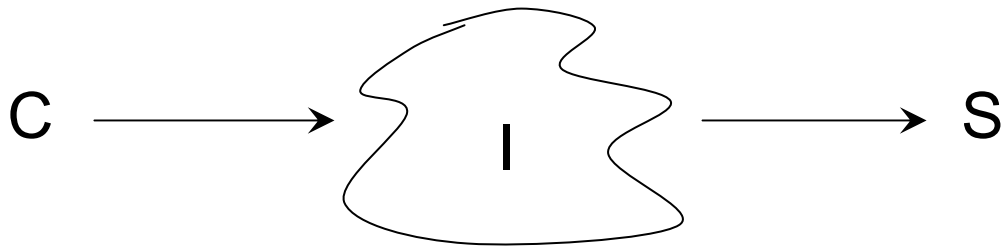
6.033 Computer System Engineering

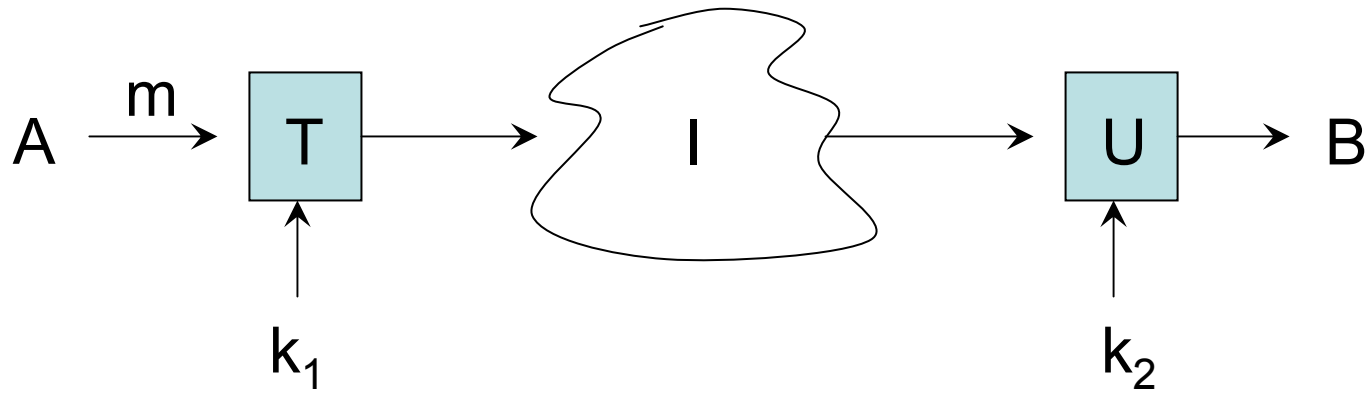
Spring 2009

Protection



1) authentication
2) authorization
3) confidentiality

Crypto



Shared key (DES)
$k_1 = k_2$

Public key (RSA)
$k_1 \neq k_2$

Security Primitives → sign, verify

Security Primitives → encrypt, decrypt

Pub. Key

A → B

$\{m\}^{kApriv}$
sign

$\{m\}^{kBpub}$
encrypt

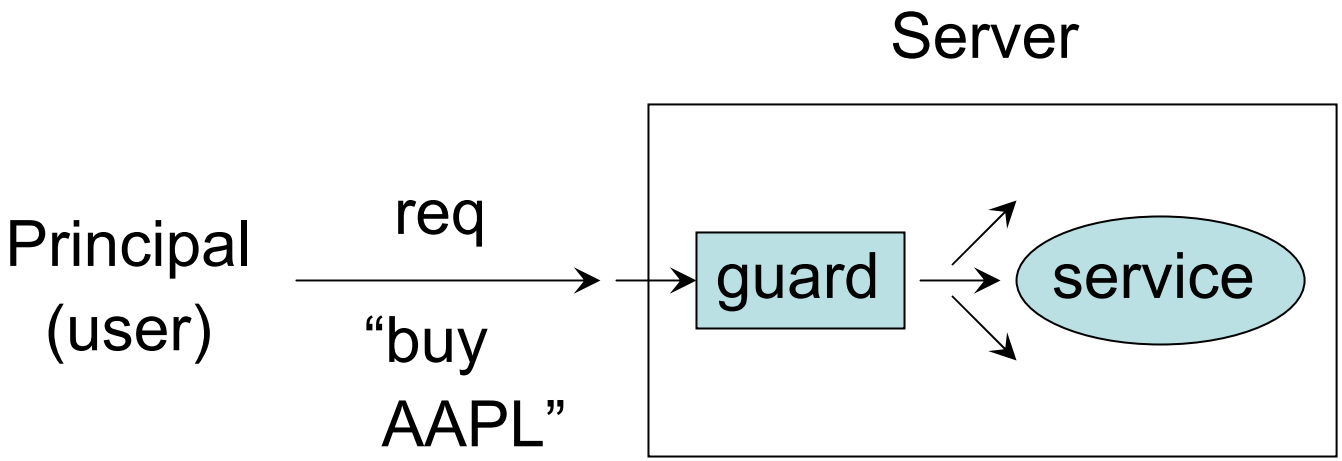
hard to build

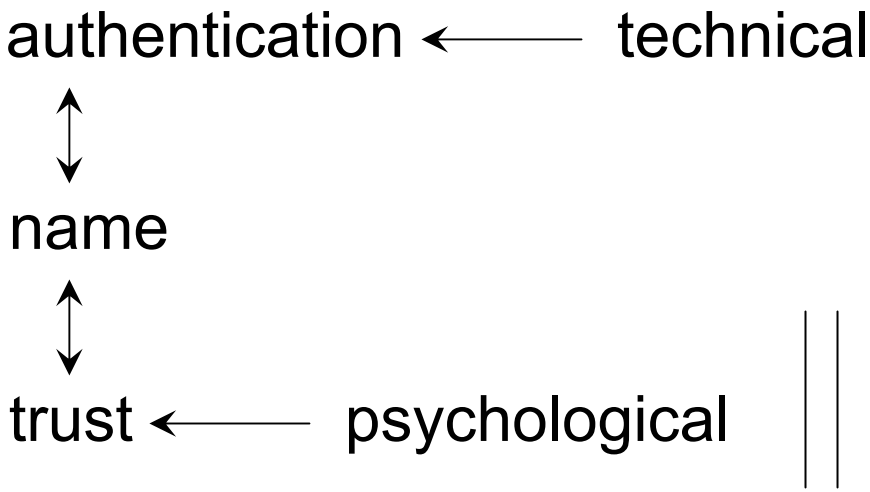
Authentication

1) Who is requesting?
   (same principal as before)

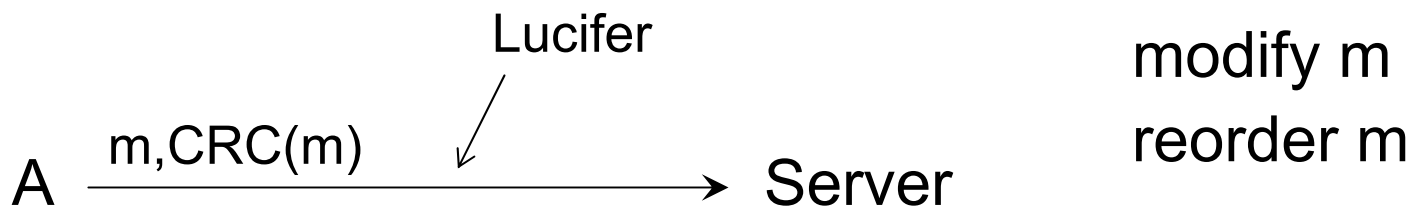
2) Mesg that was sent = mesg recv.

Model




authentication
technical
name
trust
psychological

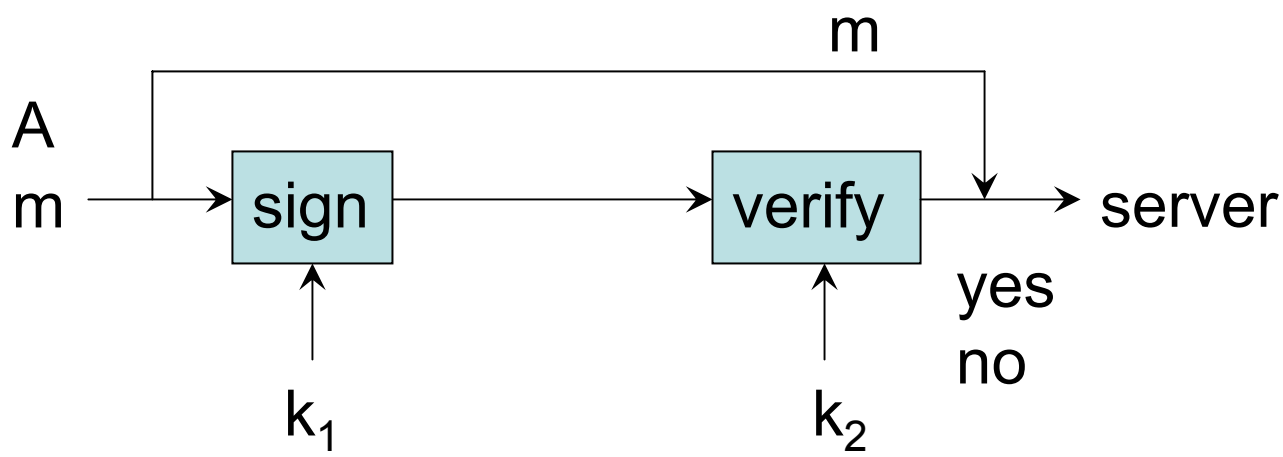
Integrity ≠ Authenticity ≠ Confidentiality



"Donate $100 to Save the Whales."

- One time pad → no!
- CRC

↳ checksum dependent on key



Cryptographically
secure
sha-1)

$k_1 \neq k_2$ ➔ MAC

$k_1 = k_2$ ➔ signature ~ $\{hash(m)\}^{kApriv}$

Key Distribution Problem

A → B “A’s pub key is X”

certificates

CA – certificate authority

Secure Comm. Channel

Use pub. key to authenticate

Exchange a shared key

Properties of crypt. Protocols

1) freshness
2) appropriate
3) forward secrecy

Attacks

- crypto
- replay
- impersonation