Protection

1) authentication
2) authorization
3) confidentiality
Crypto

\[ A \xrightarrow{m} T \xrightarrow{k_1} I \xrightarrow{k_2} U \xrightarrow{B} \]

Shared key \( k_1 = k_2 \) (DES)

Public key \( k_1 \neq k_2 \) (RSA)
Security Primitives

Pub. Key

A → B

\{m\}_{k_{\text{priv}}}^{k_{\text{priv}}} \quad \text{sign}

\{m\}_{k_{\text{pub}}}^{k_{\text{pub}}} \quad \text{encrypt}

hard to build
Authentication

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

2) Mesg that was sent = mesg recv.
Principal (user) req "buy AAPL"
authentication ← technical
↑
↓
name
↑
↓
trust ← psychological
Integrity ≠ Authenticity ≠ Confidentiality

A \xrightarrow{m,\text{CRC}(m)} \text{Server} \xleftarrow{\text{Lucifer}} \text{modify m reorder m}

“Donate $100 to Save the Whales.”

- One time pad → no! → checksum dependent on key
- CRC
A

\[ m \rightarrow \text{sign} \]

\[ k_1 \]

\[ m \rightarrow \text{verify} \]

\[ k_2 \]

\[ \text{server} \]

yes

no

Cryptographically secure (sha-1)

\[ k_1 \neq k_2 \Rightarrow \text{MAC} \]

\[ k_1 = k_2 \Rightarrow \text{signature} \]

\[ \{\text{hash}(m)\}^{k_{A \text{priv}}} \]
Key Distribution Problem

A $\rightarrow$ 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