CLOUD COMPUTING CONCEPTS

with Indranil Gupta (Indy)

SECURITY

Lecture B

BASIC CRYPTOGRAPHY CONCEPTS

Basic Security Terminology

- **Principals**: processes that carry out actions on behalf of users
  - Alice
  - Bob
  - Carol
  - Dave
  - Eve (typically evil)
  - Mallory (typically malicious)
  - Sara (typically server)

Keys

- Key = sequence of bytes assigned to a user
  - Can be used to “lock” a message, and only this key can be used to “unlock” that locked message

Encryption

- Message (sequence of bytes) + Key →
  (Encryption) →
  Encoded message (sequence of bytes)
- Encoded Message (sequence of bytes) + Key →
  (Decryption) →
  Original message (sequence of bytes)
- No one can decode an encoded message without the key

Two Cryptography Systems

I. Symmetric Key systems:

- K_A = Alice’s key; secret to Alice
- K_{AB} = Key shared only by Alice and Bob
- Same key used to both encrypt and decrypt a message

•E.g., DES (Data Encryption Standard): 56 b key operates on 64 b blocks from the message

Two Cryptography Systems (2)

II. Public-Private Key systems:

- K_{Apriv} = Alice's private key; known only to Alice
- K_{Apub} = Alice's public key; known to *everyone*
- Anything encrypted with K_{Apriv} can be decrypted only with K_{Apub}
- Anything encrypted with K_{Apub} can be decrypted only with K_{Apriv}

- RSA and PGP fall into these categories
  - RSA = Rivest Shamir Adleman
  - PGP = Pretty Good Privacy
  - Keys are several 100s or 1000s of b long
  - Longer keys => harder for attackers to break
  - Public keys maintained via PKI (Public Key Infrastructure)

Public-Private Key Cryptography

- If Alice wants to send a secret message M that can be read only by Bob
  - Alice encrypts it with Bob’s public key
  - $K_{Bpub}(M)$
  - Bob only one able to decrypt it
  - $K_{Bpriv}(K_{Bpub}(M)) = M$
  - Symmetric too, i.e., $K_{Apub}(K_{Apriv}(M)) = M$

Shared/Symmetric vs. Public/Private

- Shared keys reveal too much information
  - Hard to *revoke* permissions from principals
  - E.g., group of principals shares one key

    → want to remove one principal from group

    → need everyone in group to change key
- Public/private keys involve costly encryption or decryption
  - At least one of these 2 operations is costly
- Many systems use public/private key system to generate shared key, and use latter on messages

Next

- How to use cryptography to implement security mechanisms