
Homework 10

Operating Systems

CS 3430

Sarah Diesburg

Access Control List vs Capability List

- **Access Control List** - Stores all permissions for all users with each object
 - **Capability List** – Stores all objects a process can touch

 - Access control list is easier for file systems
 - Easy to know who can access the file when doing permission checks on a per-file basis
-

Public Key Encryption

- I send you a message:
Encrypt(KEYsarah_private, “Homework is due tomorrow”)

Public Key Encryption

- I send you a message:
Encrypt(KEYsarah_private, “Homework is due tomorrow”)
- This is **authentication** – everyone can read the message with my public key, but ***only I*** could have created it.
- You know it came from me!

Public Key Encryption

- You send me a message:
Encrypt(KEYsarah_public,
Encrypt(KEYmy_private, “I need another day.”))

Public Key Encryption

- You send me a message:
Encrypt(KEYsarah_public,
Encrypt(KEYmy_private, “I need another day.”))
- Both **authentication and secrecy**. Only you can create this message created with your private key, but only I can read it because the whole thing is encrypted with my public key.

Pentagon Traffic Analysis

- Another example – Can tell that it must be close to a project deadline due to the number of connections to the class Linux server

Networks

- Describe one advantage of point-to-point networks over broadcast networks

Networks

- Describe one advantage of point-to-point networks over broadcast networks
 - No collisions (or arbitration) needed
 - Greater aggregate bandwidth than a single link
 - Network capability can be updated incrementally