CSCI-3753: Operating Systems
Fall 2018

Anh Nguyen

Department of Computer Science

University of Colorado Boulder

Announcements

- PS5 will be available by the end of today.

- Final exam format
  - Total duration: 1 hour 15 minutes
  - Method:
    - Write on paper for the first 1 hour

      → Proof of submission/attendance
    - Transfer the results achieved on paper to Moodle opened for the last 15 minutes

➔ Bring your LAPTOP !!!

Problem Set #3

Solution of Question 3

- Suppose on-demand paging is employed in addition to TLB caching.
  - The time for a TLB hit **T = 1 ns**
  - A memory read **M = 10 ns**
  - A disk read **D = 10 ms**
  - The probability of a TLB hit **P_TLB = 90%**
  - The probability of a page fault given a TLB miss **P = 0.001**

- What is the probability of a TLB miss?

$$\mathbf{1} - \boldsymbol{P_{TLB}} = 1 - 0.9 = 0.1$$

Solution of Question 3

- Suppose on-demand paging is employed in addition to TLB caching.
  - The time for a TLB hit **T = 1 ns**
  - A memory read **M = 10 ns**
  - A disk read **D = 10 ms**
  - The probability of a TLB hit **P_TLB = 90%**
  - The probability of a page fault given a TLB miss **P = 0.001**

- What is the probability of a NO page fault?

$$\boldsymbol{P_{TLB} + (1 - P_{TLB})(1 - P)}$$
$$= 0.9 + (1 - 0.9)(1 - 0.001)$$
$$= 0.9 + 0.0999 = 0.9999$$

Solution of Question 3

- Suppose on-demand paging is employed in addition to TLB caching.
  - The time for a TLB hit **T = 1 ns**
  - A memory read **M = 10 ns**
  - A disk read **D = 10 ms**
  - The probability of a TLB hit **P_TLB = 90%**
  - The probability of a page fault given a TLB miss **P = 0.001**

- What is the calculated average memory access time in Nano seconds?

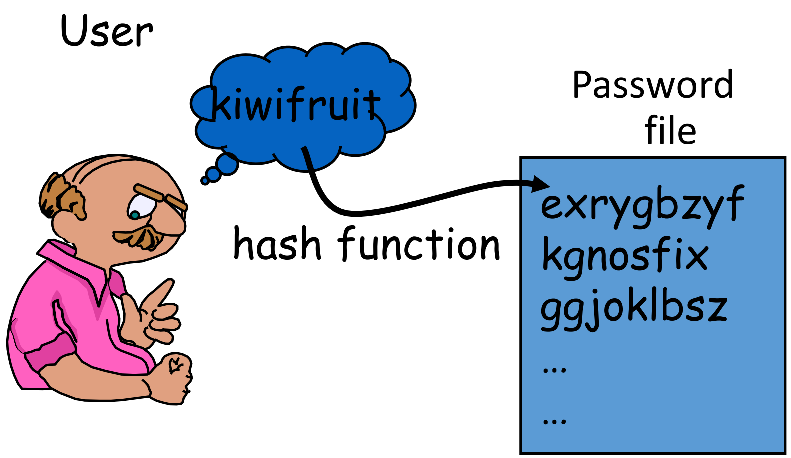
$$\boldsymbol{P_{TLB}(T+M)+(1-P_{TLB})(1-P)(2M)} \\ \boldsymbol{+(1-P_{TLB})(P)(2M+D)} = 1011.9\,ns$$

Week 14: Security

6 Main Areas of Security

- Authentication – proving you are who you say you are, e.g. passwords (most common!), biometrics
- Authorization – managing access to resources, e.g. files
- Confidentiality – only allow authorized viewing of data - encrypting files and communication
- Data Integrity – detecting tampering with digital data
- Non-repudiation – proving an event happened
- Availability – ensuring a service is available (despite denial of service attacks)

Authentication



- User authentication
  - Password authentication
  - Biometrics
  - Token-based authentication
  - Challenge-response authentication protocols
- Authentication in distributed systems (multi service providers/domains)
  - Single sign-on, Microsoft Passport
  - Trusted Intermediaries

Authorization

- First authenticate a user with a login password
- Then, OS must determine what files/services the user/process is authorized to access

→ Object and access rights are stored in an access matrix.

- Access control list (ACL)
  - All access permissions to a file are stored in the file header, forming an ACL for the file
- Capability list
  - All access permissions for a user are stored with D4's account information, forming a list of capabilities for the user

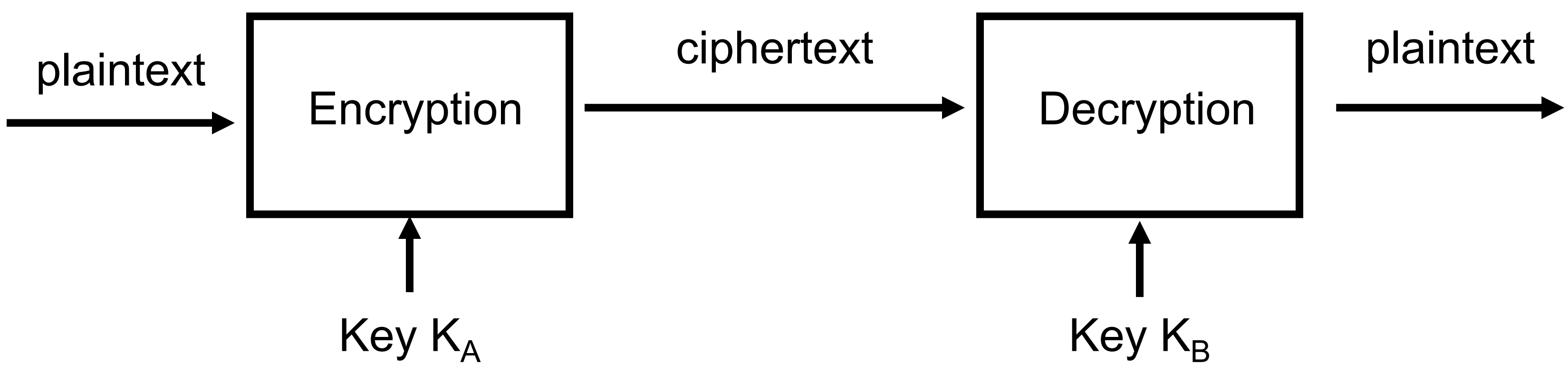
Objects

Domains/users

	file F1	file F2	file F3
D1	read		read
D2		owner read	
D3		read	execute
D4	read, write		read, write

Confidentiality

- Encrypt
  - Files to protect the confidentiality of the data
  - Communication messages to protect the confidentiality of the messages
- Only designated decryptors can view the data



Confidentiality

- Symmetric key cryptography: $K_A = K_B$
  - Use the same key for encryption & decryption
  - Has been used since the times of the Romans
  - Also called secret key or private key cryptography
  - AES (Advanced Encryption Standard) uses symmetric key cryptography

  - Encrypted file systems use symmetric key cryptography
    - EFS (Encrypting File System for Windows)
    - and EncFS (for Linux, uses FUSE)

  - Stored in plaintext in a file in an encrypted form

Confidentiality

- Public key cryptography
  - Emerged in the 1970s, invented by Diffie and Hellman (and Merkle)
  - Endpoints exchange public quantities with each other
  - Each endpoint then calculates its symmetric key from these publicly exchanged quantities
    - The symmetric keys calculated are the same
  - Even though an attacker could eavesdrop on all the public communications, it cannot calculate the symmetric key!
  - This solves the classic symmetric key distribution problem (with a caveat explained later), and was the foundation for public key cryptography

Week 14 – Checklist

- ❑ Announcements
- ❑ Review PS3 and Security
- ❑ Do FCQ & the quiz