2018/12/11

기말 과제

- 프로세스간 메시지 송/수신 암호화 -

발표자: 컴퓨터 공학과 16학번
권 순 홍(201621110)

목차

- 개요
- 관련 기술
- 아키텍쳐
- 주요 동작 방식

Overview

- 프로세스는 서로 독립되어 있음
- 프로세스간 통신을 위해 통신 설비가 중시됨
  - Message Queue를 이용한 통신
- 프로세스간 안전한 통신이 요구됨에 따라 메시지 암호화에 따라 안전한 통신 수립
  - 암호 알고리즘 사용

관련 기술

- 프로세스간 통신 설비
  - Message Queue
    - 프로세스간 데이터를 메시지 형태로 전송하는 통신 도구
    - FIFO 타입의 데이터 전송을 지원
    - 관련 시스템 호출 함수
      - msgget()
        - 메시지 큐 생성
      - msgsnd()/msgrcv()
        - 메시지 전송 및 수신
      - msgctl()
        - 메시지 큐 제어

관련 기술

- 암호 알고리즘
  - 암호화 및 복호화를 수행하는 알고리즘
    - e.g., DES, AES, RC4
  - AES(Advanced Encryption Standard)
    - 대칭 암호 알고리즘
    - 암/복호화 키가 같음
    - 128~256 비트 키를 사용

기능

- 프로세스들 간에 이산적인 양의 데이터 송수신 가능
- 모든 프로세스에서 접근 가능하도록 구성되어 있음
- 해당 식별자는 아는 모든 프로세스가 동일한 메시지 큐에 접근하여 메시지 공유 가능

아키텍쳐

- 아키텍쳐

```
#include <openssl/aes.h>

/* AES Encrypt Process */
bool encrypt_block(unsigned char* cipherText,
unsigned char* plainText, unsigned char* key)
{
    AES_KEY encKey;


    if (AES_set_encrypt_key(key, 128, &encKey) < 0)
        return false;

    AES_encrypt(plainText, cipherText, &encKey);

    return true;
}
```

Message Structure

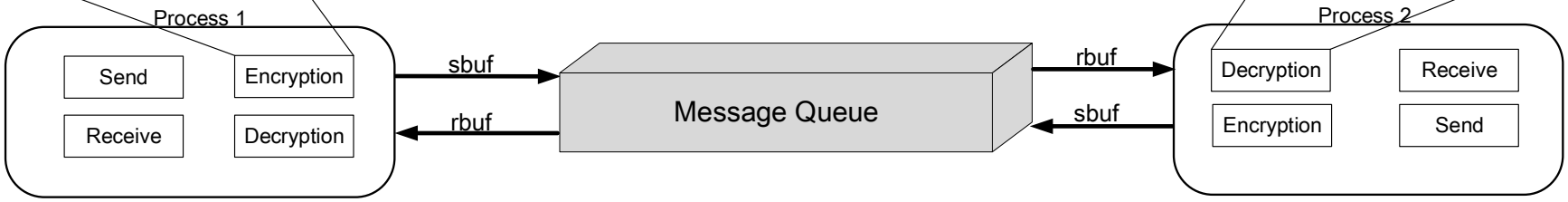
```
typedef struct msgbuf {
        long    mtype;
        char    mtext[MSGSZ];
} message_buf;
```

```
#include <openssl/aes.h>
 /* AES Decrypt Process */
bool decrypt_block(unsigned char* cipherText,
unsigned char* plainText, unsigned char* key)
{
    AES_KEY decKey;


    if (AES_set_decrypt_key(key, 128, &decKey) < 0)
        return false;

    AES_decrypt(cipherText, plainText, &decKey);

    return true;
}
```



If process 1 press 'close', the connection is terminated: hi
Process 1: hi
Process 2: hi
If process 1 press 'close', the connection is terminated: close

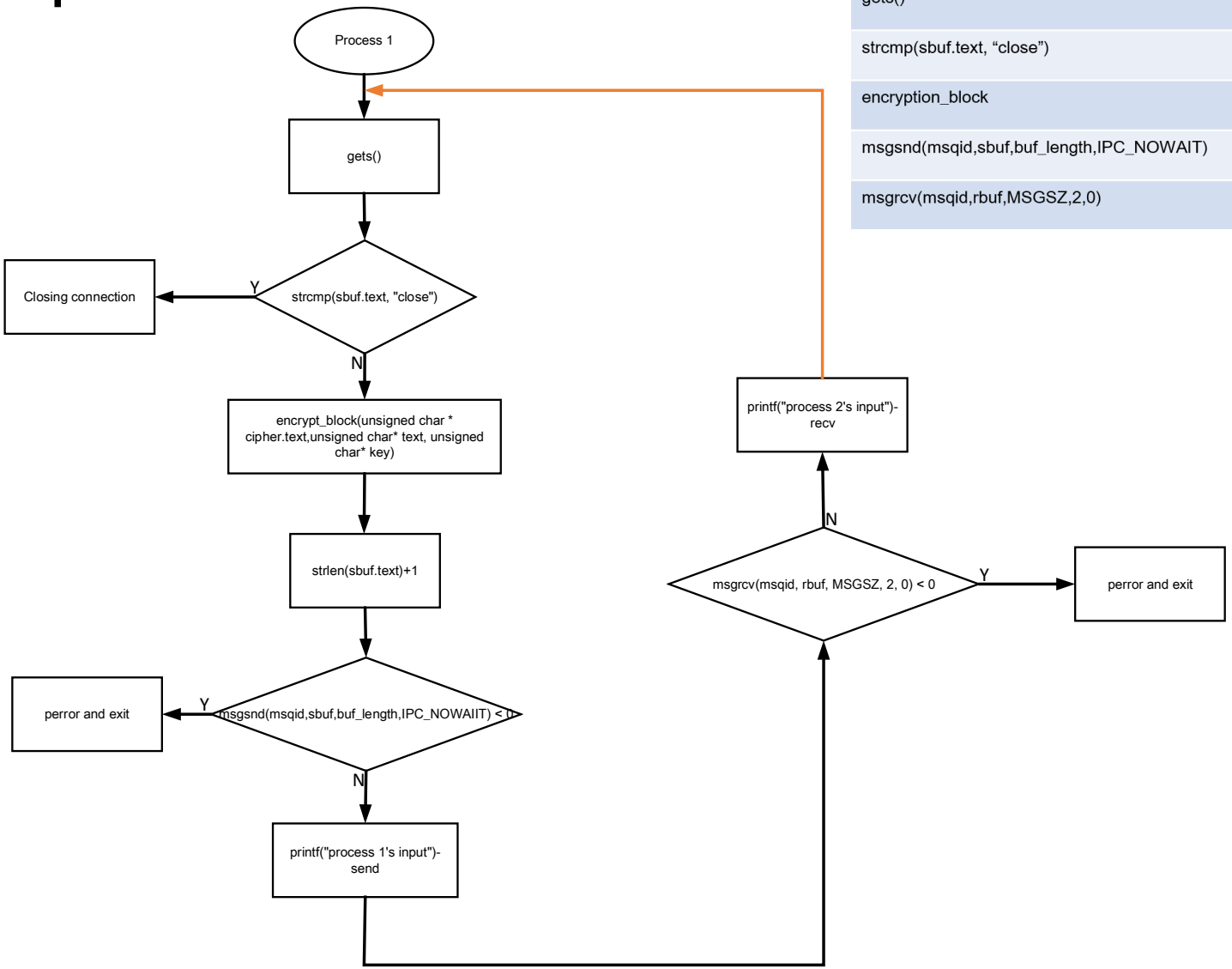
Close connection

Process 1: hi
If you process 2 press 'close', the connection is terminated: hi
Process 1: hi
Process 2: hi
If you process 2 press 'close', the connection is terminated:close

Close connection

주요 동작 방식

- process 1 동작



함수	정의
gets()	메시지 입력
strcmp(sbuf.text, “close”)	메시지 문자열 비교(프로세스간 연결 종료를 위함)
encryption_block	메시지 암호화 함수
msgsnd(msqid,sbuf,buf_length,IPC_NOWAIT)	송신 메시지 검사
msgrcv(msqid,rbuf,MSGSZ,2,0)	수신한 메시지 검사

주요 동작 방식

- process 2 동작

함수	정의
decrypt_block	메시지 복호화 함수
msgrcv(msqid,rbuf,MSGSZ,1,0)<0	수신한 메시지 검사
gets()	메시지 입력
strcmp(sbuf.text, “close”)	메시지 문자열 비교(프로세스간 연결 종료를 위함)
msgsnd(msqid,sbuf,buf_length,IPC_NOWAIT)<0	송신 메시지 검사