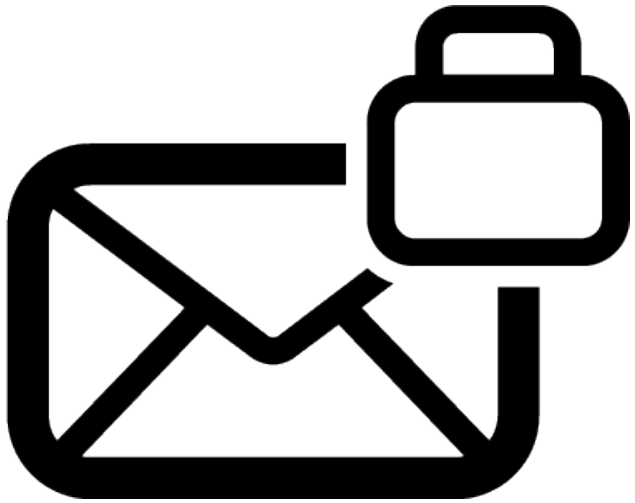
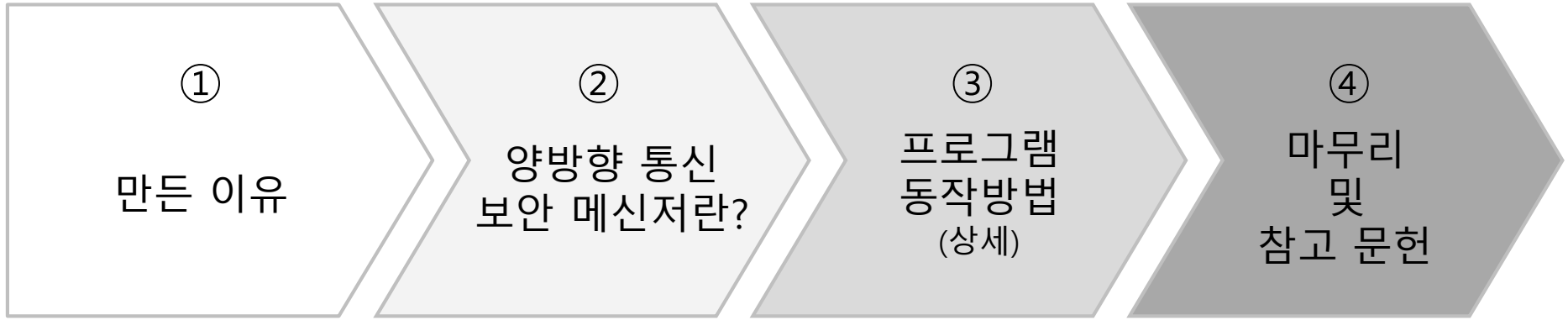


양방향 통신 보안 메신저

팀장 : 1771469 이광헌
조원 : 1094017 배재현
조원 : 1771075 나관우

목차



①-1 스마트폰 해킹 피해
①-2 중간자 공격
①-3 피해사례

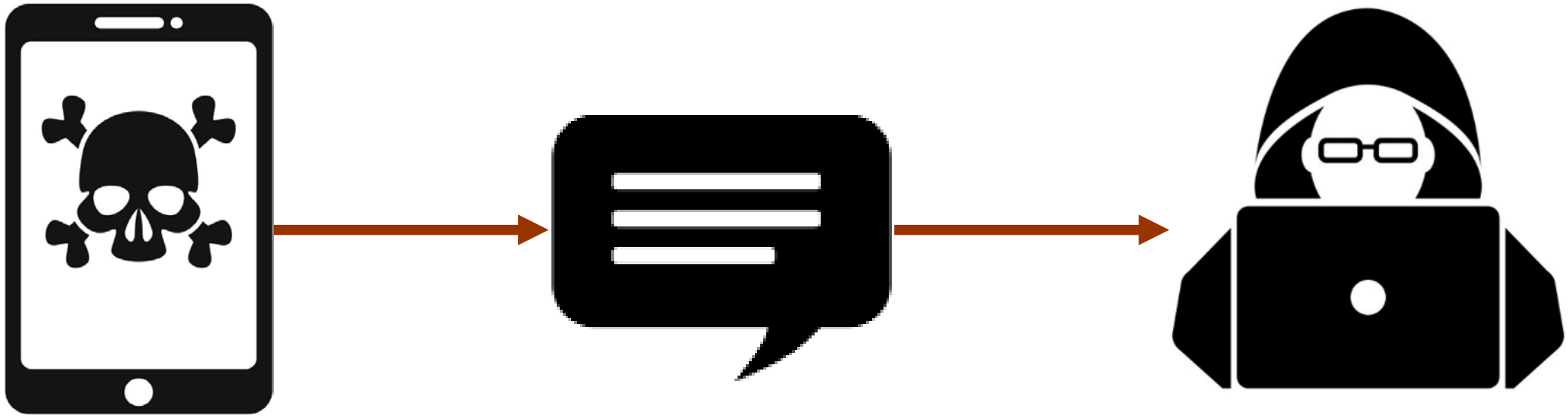
②-1 특징
②-2 프로그램 동작 방법

③-1 진행 과정
③-2 통신 시작
③-3 통신 진행
③-4 LEA 사용 이유
③-5 통신 종료

④-1 정리
④-2 스케줄 및 역할 분담
④-3 참고 문헌
④-4 Q&A

① 만든 이유

①-1 스마트폰 해킹

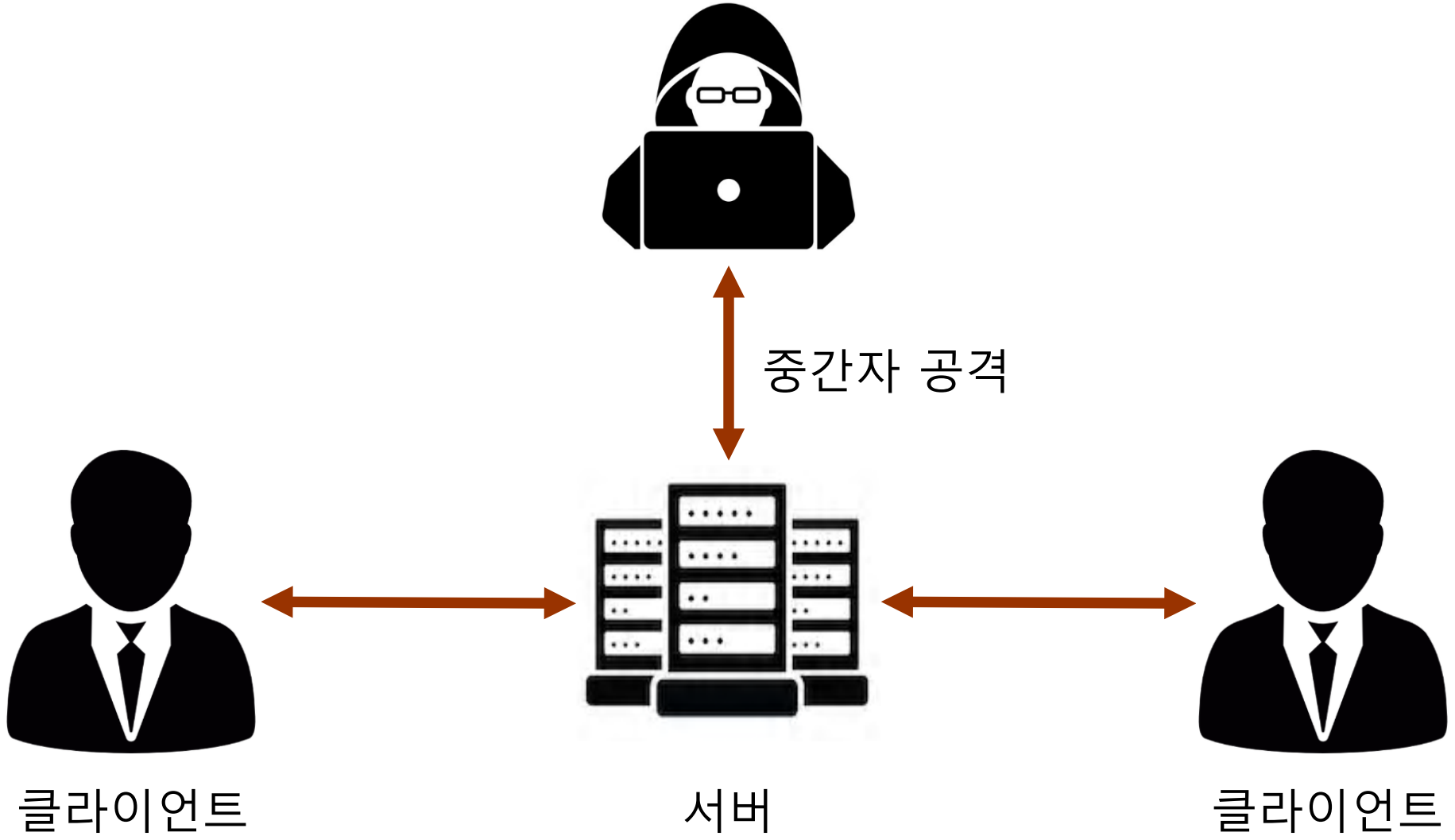


스마트폰 해킹

채팅 내용 탈취

사생활 노출,
사회 공학 공격

①-2 중간자 공격



①-3 피해사례

2020년 1월경 주진모 카카오톡 해킹 후 유출

[뉴스컬처 김은지 기자]배우 주진모 측이 휴대전화 해킹 루머에 대해 법적대응한다.

소속사 화이브라더스코리아 측은 10일 보도자료를 통해 "각종 온라인 SNS, 모바일 메신저로 유포된 주진모와 관련해 공식입장을 알린다"며 "당사는 유포된 정황을 포함한 일련의 상황에 대해 수사기관에 정식으로 수사를 의뢰하고 법적대응을 할 방침"이라고 밝혔다.

이하 주진모 측 입장 전문

안녕하세요. 화이브라더스코리아입니다.

최근 각종 온라인 SNS, 모바일 메신저 애플리케이션을 통해 유포되고 있는 소속 배우 주진모 씨 관련하여 공식 입장 알려드립니다.

해당 사항에 대해 당사는 유포된 정황을 포함한 일련의 상황에 대해 수사기관에 정식으로 수사를 의뢰하고 강경한 법적대응을 할 방침 입니다. 따라서 위와 같은 유포 등 행위를 자제해 주시기 바랍니다.

속칭 '지라시'를 작성하고 이를 게시, 또는 유포하는 모든 행위는 법적 처벌 대상입니다. 때문에, 현재 무분별하게 배포되고 있는 관련 내용을 어떠한 경로라도 재배포 및 가공 후 유포 시 당사는 법무법인을 통해 강력하게 법적인 조치를 취하고 책임을 물을 예정입니다.

http://nc.asiae.co.kr/view.htm?idxno=2020011015030506388

② 양방향 통신 보안 메신저란?

②-1 특징

기본적인 메신저의 기능에 더불어

메시지 블록암호화(LEA 알고리즘 사용)를 통해 중간자 공격이 불가능하게 하고

대화가 끝남과 동시에 채팅기록, 로그를 모두 삭제하여

해킹으로 인한 사생활 누출, 사회 공학 공격 등을 불가능하게 만든

비밀 보안 메신저

②-2 프로그램 동작 방법

1. 각 클라이언트는 로그인 후 클라이언트 끼리 연결

2. 서버는 각각의 클라이언트에게 KEY값 전달

3. 서버가 전달한 KEY값을 이용해서 각 메시지 블록암호화 후 통신
(LEA 암호화 알고리즘 사용)

4. 채팅 종료 시 클라이언트 및 서버 컴퓨터 내의 메시지 및 로그 삭제

③ 프로그램 동작 방법(상세)

③-1 진행 과정

③-2 통신 시작

클라이언트
로그인

방 생성

대기

상대방
참가 시

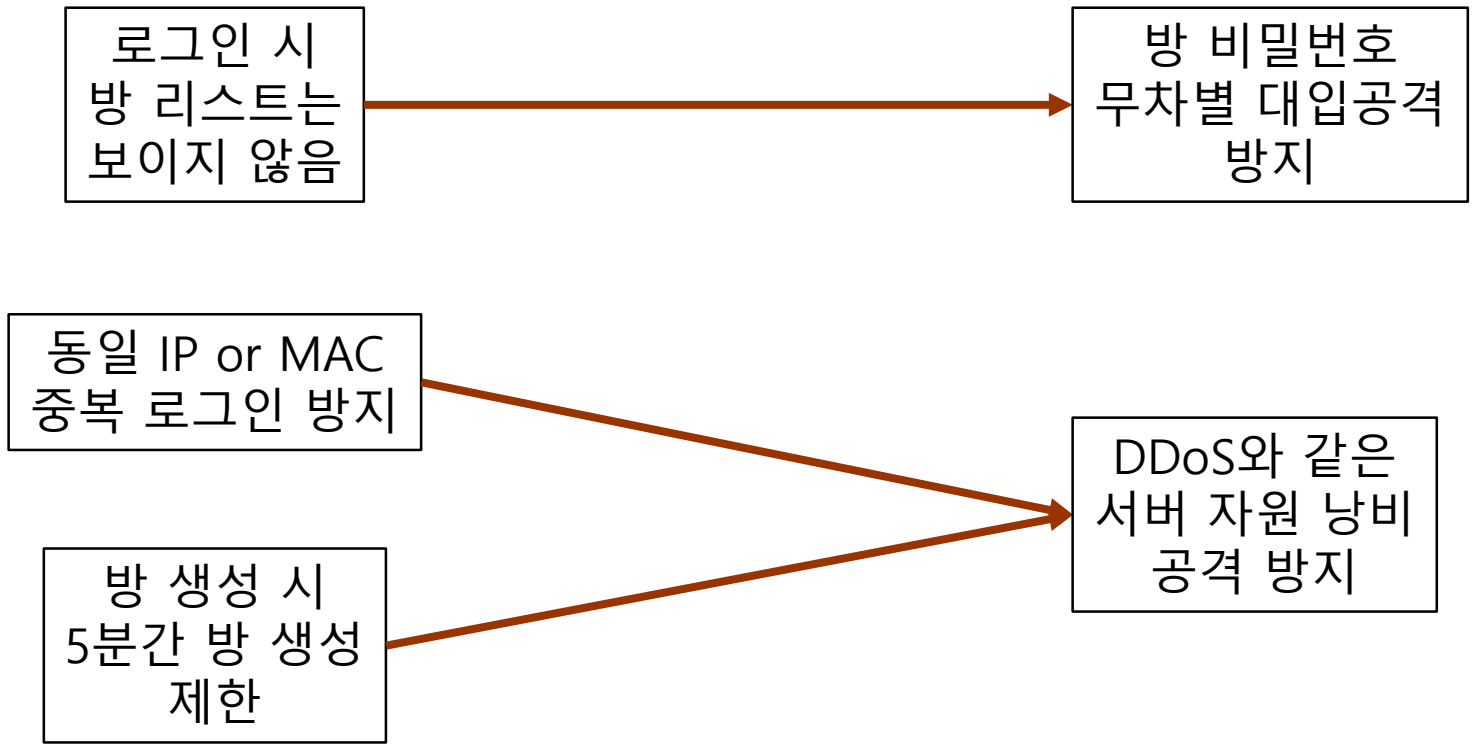
시작

방 이름
PW

방 참가

③-2 통신 시작

적용된 보안 기법



③-3 통신 진행

서버는 클라이언트에게
KEY값 전달.
KEY값은 서버에서
무작위로 생성

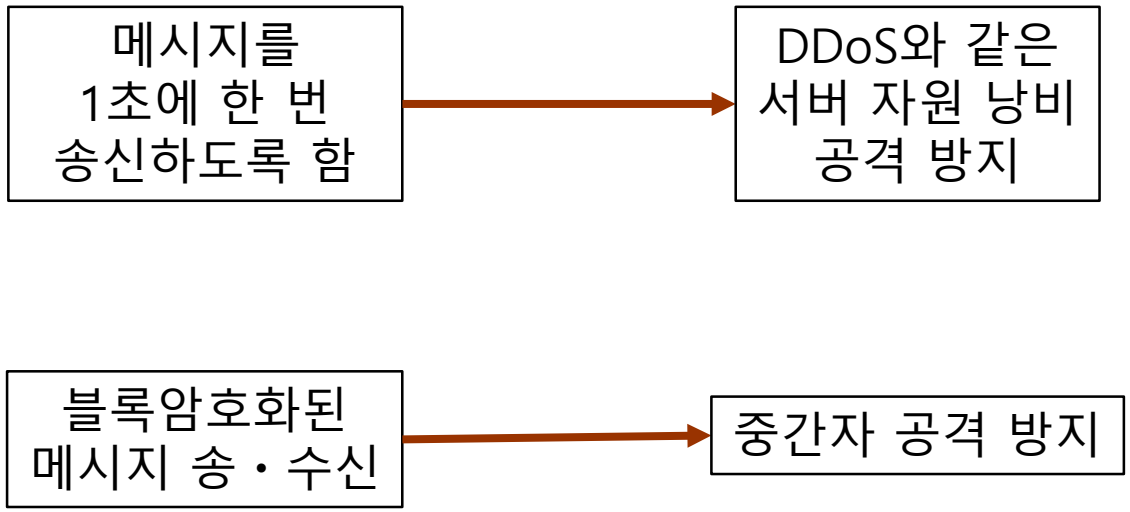
KEY값은 생성된 후
방의 비밀번호와
XOR 암호화 되어 전달

③-3 통신 진행

서버에서 전달받은 KEY와
LEA 암호화 알고리즘을 이용하여
암호화된 메시지를 송・수신

③-3 통신 진행

적용된 보안 기법

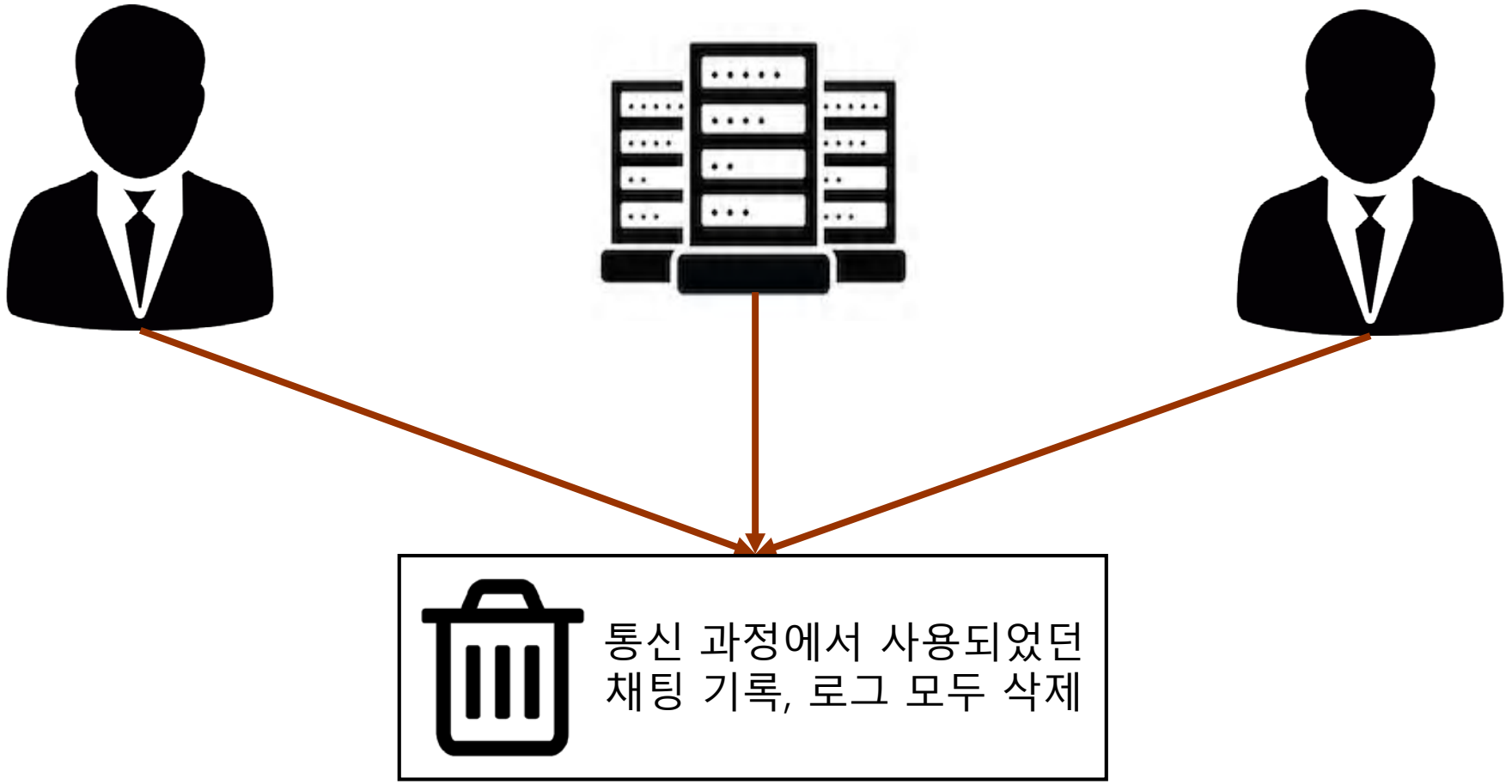


③-4 LEA 사용 이유

LEA란?	LEA 사용 이유	LEA 중 OFB 모드 사용
Lightweight Encryption Algorithm. 국가보안기술연구소에서 개발. 빅데이터, 클라우드 등의 고속 환경 및 모바일기기 등 경량 환경에서 기밀성을 제공하기 위해 개발된 128비트의 데이터 블록 암호화 기술.	SBOX 사용을 피하고 ARX 형태로 구현하여 AES보다 2배정도 빠르고 기존 경량화 암호인 HIGHT보다 더욱 안정적이어서 선택하였음.	한 단계 앞의 암호문 블록과 평문 블록을 XOR하여 암호문 블록을 만드는 모드. 블록보다 작은 크기의 데이터에서 동작이 가능하여 선택. 채팅의 경우 블록보다 크기가 작은 경우가 많으므로 적합함.

http://wiki.hash.kr/index.php/LEA
https://namu.wiki/w/LEA

③-5 통신 종료



④ 마무리 및 참고 문헌

④-1 정리

양방향 통신 보안 메신저 → 메시지 블록암호화 채팅 기록 및 로그 삭제 → 중간자 공격 방지 해킹으로 인한 데이터 누출 방지 → 강력한 비밀 보안 메신저

단순 목적의 사용?

범죄에 악용?

판단은 사용자의 몫

④-2 스케줄 및 역할 분담

스케줄		역할 분담	
주차	활동	이름	역할
3주차	제안서 제출	이광헌	프로젝트 진행 및 프로그램 개발 보조
4주차~8주차	프로그램 개발(텍스트 채팅)	배재현	발표 및 발표 자료 디자인
9주차~11주차	프로그램 개발(파일 첨부 및 인터페이스 수정)	나관우	프로그램 개발 총괄
12주차~14주차	취약점 테스트 및 인터페이스 최종 수정		
15주차	결과물 발표 및 보고서 제출		

④-3 참고 문헌

주진모 카카오톡 해킹 관련 기사

해킹 피해 주진모, '지라시'에 법적대응 - 뉴스컬쳐
http://nc.asiae.co.kr/view.htm?idxno=2020011015030506388

LEA 관련 자료

LEA - KISA 암호이용활성화
https://seed.kisa.or.kr/kisa/algorithm/EgovLeaInfo.do

LEA - 해시넷
http://wiki.hash.kr/index.php/LEA

LEA - 나무위키
https://namu.wiki/w/LEA

THANK YOU!
ANY QUESTION?