하이브리드 기법과 중간자 공격

201103002
김경민

목 차

1. 하이브리드 암호체계

2. 중간자 공격

하이브리드 기법의 용어 설명

하이브리드 기법은 합성 암호 체계(hybrid cryptosystem)라고 불림
공개키와 대칭키의 각자의 단점을 보완하고자 만들어진 시스템

합성암호체계

대칭키 암호화의 장점

빠르고, 대용량 데이터를 처리하기에 적합

공개키 암호화의 장점

커다란 키공간을 갖고 있어서 보안성을 가지고 있음

합성암호체계(Hybrid cryptosystem)

암호화 되는 과정

대칭키로 암호화

암호화된 메시지

의사난수 발생기

세션키

수신자의 공개키

공개키 암호로 세션 키를 암호화

암호화 된 세션 키

결 합

복호화 되는 과정

메시지 복호화

분 할

세션키 복호화

대칭키로
암호화된 메시지

공개키로
암호화된 세션키

수신자의
개인키

세션키를 복호화

대칭키로
암호화된 메시지
복호화

세션 키

사용되는 암호화 기법

1)의사난수 생성기(세션키 발생)

2)대칭 키 암호

3)공개 키 암호

합성 암호 체계 사용하는 곳

PGP (Pretty Good Privacy)

인터넷에서 전달하는 전자우편을 다른 사람이 받아 볼 수 없도록 암호화하고, 받은 전자우편의 암호를 해석해주는 프로그램

중간자 공격

Man-in-the-Middle Attack

디피-헬먼의 키교환

1)1976년에 최초로 발표된 공개키 암호 기법

2)공개키를 교환하여 상호간에 사용할 비밀키 생성

3)비밀키는 암호문의 생성 및 평문의 복구를 위한 암호 및 복호키로 사용

4)중간자 공격에 대한 취약함

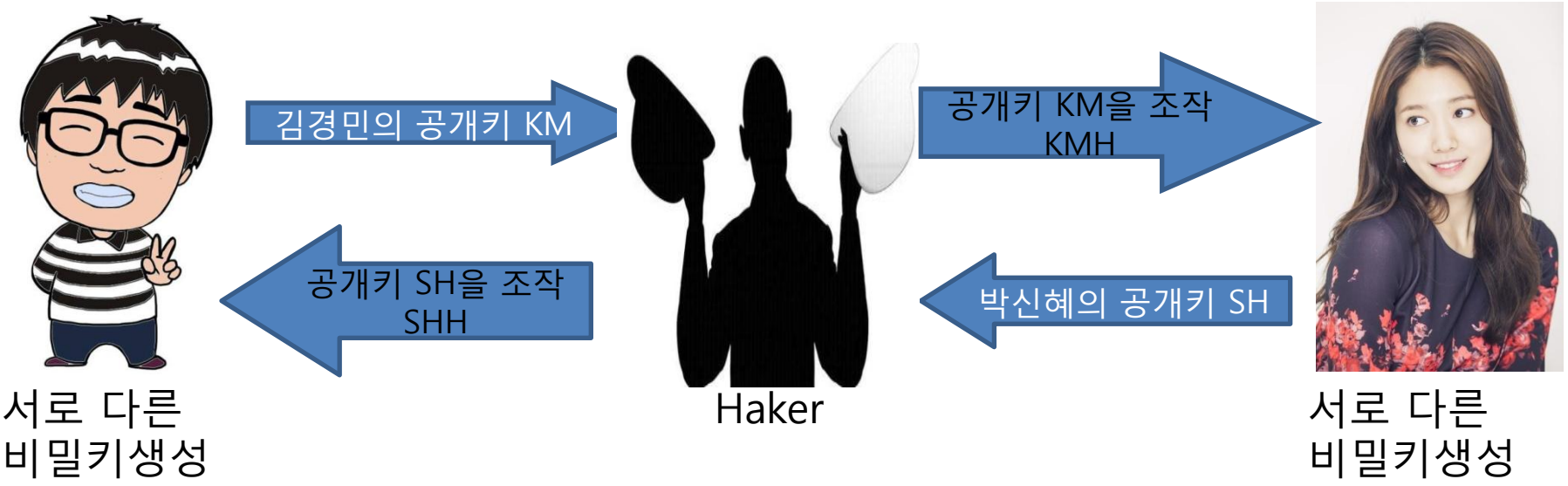
비밀키생성

김경민의 공개키 KM

박신혜의 공개키 SH

비밀키생성

중간자 공격



결국 서로 다른 비밀키를 생성하게 됨

중간자 공격 해결 방안

김경민 공개키 KM & 인증이 된 전자서명

박신혜 공개키 SH & 인증이 된 전자서명

전자서명 확인 후 비밀키 생성

전자서명 확인 후 비밀키 생성

공격자에 의한 공개키의 변조를 방지하기 위하여
전자 서명된 공개키를 상호 교환