네트워크 보안

이중 암호화 체계를 이용한 네트워크 보안 시스템

Keyword	보안 암호, 공개키 암호, 아이디 기반 암호, IoT, 홈 네트워크, 클라우드		
기술보유 기관	한국과학기술정보연구원 (KISTI)	기술판매형식	기술협력, 라이센스
연구 책임자	박 상 배	기술 완성단계(TRL)	파일롯 규모 시작품 제작 및 성능 평가(6단계)

기/술/개/요

본 기술은 공개키 암호화 시스템 및 사용자 ID 기반 암호화 시스템을 혼합한 이중 암호화 체계를 구성함으로써, 네트워크 연결의 보안을 향상시키는 기술

기존 기술의 문제점

1. 공개키 암호화 시스템의 인증서 관리 문제
   - 종래 공개키(Public Key Infrastructure;PKI)를 기반으로 한 암호화 시스템의 경우 암호화 통신을 위해 통신 대상간에 인증서를 사전 교환해야 함
2. 공개키 암호화 시스템의 상호 동등한 관계 신뢰 모델
   - 종래 공개키 기반의 암호화 시스템은 통신 대상들이 모두 동등한 신뢰 모델로 하위 종속적인 통신 대상들에 대해 적용하기 어려움
3. 아이디 기반 암호의 단일 적용의 어려움
   - 아이디에 대한 개인키 발급을 위해 안전한 통신 채널이 확보되어야 하고, 표준화 및 기반 기술의 보급이 부족함

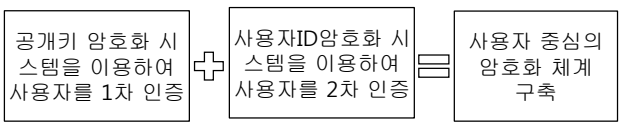
기술 내용 및 차별성

기술 내용 차별성

공개키 기반 암호화 시스템 및 사용자 ID 기반 암호화 시스템을 함께 적용하여 신뢰성 향상 및 사용자 편의성 향상

기술 내용

- 공개키 기반의 암호화 시스템을 이용하여 사용자를 1차 인증하고 안전한 채널 확보
- 사용자의 ID 기반의 암호화 시스템을 이용하여 사용자의 ID를 기반으로 사용자를 2차 인증



차별성

- 이중 암호 체계를 적용함으로써, 사용자 보안을 향상
- 사용자 ID기반 암호화 시스템을 적용하여, 사용자 중심의 암호화 체계 구축 가능
- 사용자 ID기반 암호화 시스템을 적용하여, 제한적인 통신 대역폭을 가진 환경에서도 암호화 인증이 가능

주요기술구성 및 구현방법

주요기술구성

① 공개키 기반 사용자 1차 인증 단계	②사용자 ID 기반 사용자 2차 인증 단계	③ 네트워크 기기와 통신 및 제어 단계
공개키 기반의 암호화 시스템을 이용하여 사용자를 인증	사용자 ID 기반의 암호화 시스템을 이용하여 사용자를 2차 인증	사용자가 네트워크 기기와 통신하여 제어

구현예

#1) 홈 네트워크 서버를 통해 연결된 다양한 가전제품을 제어하는데 적용

- 공개키 기반의 암호화 시스템을 이용하여 사용자를 1차 인증
  - 사용자가 홈 네트워크 서버에 1차 인증을 시도하면, 홈 네트워크 서버에서는 공개키 암호화 시스템을 이용하여 사용자를 인증함으로써, 사용자가 홈 네트워크 서버에 접속가능하도록 함

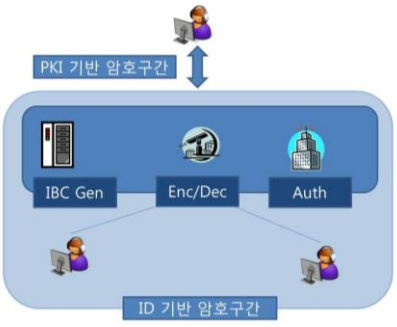
- 사용자 ID 기반의 암호화 시스템을 이용하여 사용자를 2차 인증
  - 홈 네트워크 서버가 1차 인증이 완료된 사용자로부터 사용자 ID를 수신하여 사용자 ID 기반의 암호화 시스템을 통해 2차 인증을 수행함으로써, 사용자가 홈 네트워크 서버와 연결된 가전제품에 접속가능하도록 함

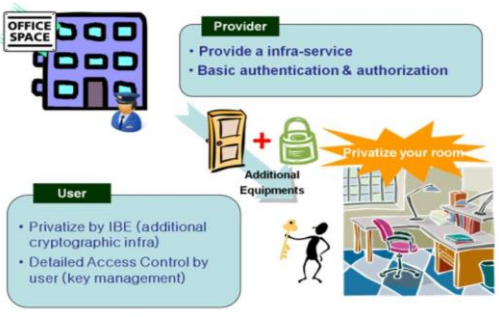
- 사용자가 홈 네트워크 서버를 통해 가전제품을 제어
  - 사용자가 냉난방기기, 냉장고, 컴퓨터, 오디오 등에 접속하여 해당 가전제품을 제어

#2) 암호화된 메시지를 전송하는데 적용

- 내부 사용자 간에는 사용자 ID 기반의 인증을 통해 메시지를 전송
  - 사용자1이 사용자2에게 메시지를 전송하는 경우, 사용자1은 사용자 2의 ID를 이용하여 메시지를 암호화한 후 전송하고, 사용자2는 자신의 ID 기반으로 생성된 개인키를 이용하여 메시지를 복호화

- 내부 및 외부 사용자 간에는 공개키 기반의 암호화와 사용자 ID 기반 암호화를 통해 메시지를 전송
  - 내부의 사용자1이 외부의 사용자2에게 메시지를 전송하는 경우, 사용자1은 사용자2에게 전송할 메시지가 있음을 알리는 메시지를 사용자2의 가상ID를 기반으로 암호화한 후 전송함
  - 사용자2에 의해 공개키 기반 인증이 수행되면, 사용자2의 ID에 따른 개인키를 이용하여 사용자2의 세션키를 복구하고, 복구된 세션키를 이용하여 PKI 기반의 공개키로 암호화된 사용자1의 메시지를 사용자2에게 전송하고, 사용자2는 PKI 기반의 개인키를 이용하여 전송된 메시지를 복호화





기술 시장 동향

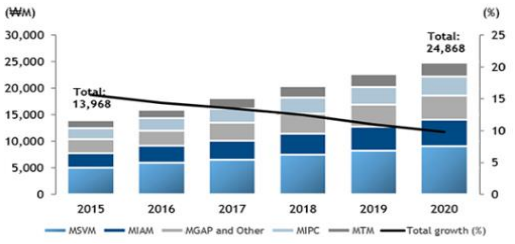
기술 동향

- **컴퓨팅과 네트워킹이 결합된 서버, 스위치** 등의 **고성능 클라우드 보안 플랫폼 기술**이 개발되고 있음
  - **클라우드 환경에서의 보안 기능의 지능화에 대한 연구**와 고**성능 보안 가상화 플랫폼 개발**이 **진행**되고 있음
  - 기존 위협 패턴 분석기반의 공격 제어 기업의 한계를 넘어서 **제품 간의 지능형 관계성 분석을 통한 클라우드 환경의 통합 보안위협 인텔리전스 기술 확보 경쟁**이 이루어지고 있음

- **국내 : NFV (Network Function Virtualization)기술을 이용한 보안 서비스 가상화 기술이 개발중임**
  - 국내의 경우 Sdsec(software-defined security)와 같은 SDN 특성에 기반한 보안 기술은 기초 연구 수준에 머물러 있으며, NFV 기술을 이용한 보안 서비스 가상화 기술이 개발 중임
- **해외 : 가상화와 소프트웨어 정의 보안 기술을 연구 및 개발**
  - 범유럽 연구개발 프로젝트인 '5GPPP'와 에릭슨 등에서5G 이동통신기술에 대한 다양한 의견을 정립 중이고, ITU-R, ARIB 등에서는 5G 이동통신에 대한 기술동향 보고서, 5G 백서 등을 발표하였음

시장 동향

- 클라우딩 환경에 대한 관심도가 증가함에 따라 네트워크 보안 요구가 급증
  - 2015년 **국내 기업용 모바일 보안 소프트웨어 시장**은 **약 140억 규모로** 추산되며, **향후 5년간 연평균 12.2%로 성장**하여 오는 **2020년 250억 규모를 형성할 것으로 전망**
  - 유·무선 네트워크 보안 품목의 세계시장 규모는 **2015년 70억 4백만 달러 규모로 추산**되며, **2018년까지 연평균 1.5% 성장**하여 **73억 23백만 달러의 시장을 형성**할 것으로 **전망**
  - **전세계 사이버보안 시장**은 '15년도 기준 754억 달러이며, '**21년까지 1,200억 달러 규모 시장**으로 **성장**할 것으로 예상됨
  - 한국 정보보안협회의 조사에 따르면, **국내 사이버 보안 기업**의 숫자는 **299개**로 **전년보다 43개가 증가**함



[유무선 네트워크 보안 시장현황 및 전망]

(단위: 백만 달러, 억 원)

구분	2013	2014	2015	2016	2017	2018	성장률(%) (2013~2018)
세계시장	6,798	6,900	7,004	7,109	7,215	7,323	1.50%
국내시장	4,482	4,734	4,999	5,279	5,575	5,887	5.60%

출처: Network Security Appliances and Software (Infonetics Research, 2015), 2015 국가정보보호백서, 국가정보원, 미래창조과학부, 방송통신위원회, 행정자치부 (2015년 4월) 등의 자료를 참고하여 전망치 추정

기술활용분야 및 권리현황

기술활용분야

기술 수요처	적용처
전자인증 업체, 사이버 보안 업체	전자인증, 사이버 보안, 인터넷뱅킹
전자 결제 솔루션 업체, 온라인 쇼핑 업체, 핀테크 업체	핀테크, 전자결제
그룹웨어 업체, SNS 서비스 업체	계정/권한관리, 메신저 및 e-mail 서비스

권리현황

-국내등록특허 9건

발명의 명칭	특허번호	비고
그리드 작업 스케줄링 및 방법	10-1092359	등록
공유 컴퓨터 리소스들에 대한 암호화 장치 및 그 방법	10-1304523	등록
네트워크 시스템의 암호화 장치 및 그 방법	10-1374196	등록

기술활용분야 및 권리현황

발명의 명칭	특허번호	비고
암호화 메시지 전송방법, 암호화 메시지 전송장치, 암호화 메시지를 전송하는 암호화 모듈 프로그램을 저장하는 저장 매체	10-1458034	등록
데이터 암호화 장치 및 데이터 암호화를 수행하는 프로그램을 저장하는 저장매체	10-1413248	등록
라이센스 관리 장치, 라이센스 관리 시스템, 라이센스 관리 방법 및 저장매체	10-1545940	등록
접근권한 제어 장치, 단말 장치를 포함하는 접근권한 제어 시스템 및 암호화 및 복호화 방법, 접근권한 제어 방법	10-1489862	등록
클라우드 서비스를 이용한 2중 백업 시스템 및 관리방법	10-1628195	등록
블록 암호를 이용한 일방향 암호 시스템	10-1613565	등록

추가 기술 정보

기술분류	네트워크 보안 >암호, 인증
시장전망	국내 기업용 모바일 보안 소프트웨어 시장은 2020년 250억원대 규모를 형성할 것으로 전망
기술문의	박상배 책임연구원(KISTI 슈퍼컴퓨팅응용실) 042-869-1041 plucky@kisti.re.kr
	한만호 실장(KISTI 기획부/성과확산실) 042-869-0945 mhh7535@kisti.re.kr
	심경식 대표(㈜SYP) 02-563-9607 shim@sypip.com