2015년 12월

15ZS1210-01-1412P

15

시큐리티 큐레이션을 제공하는 프라이버시강화형 개인정보 유통보안 핵심기술 개발

Development of core technology in privacy enhanced personal information distribution security for providing security curation

ETRI 한국전자통신연구원
Electronics and Telecommunications Research Institute

인 사 말 씀

IT 기술의 놀라운 발전과 스마트폰의 등장은 기존에 상상할 수 없었던 새로운 경험을 우리에게 선사하고 있습니다. 인간의 사회적인 활동, 경제적인 행위, 개인 생활에 있어 IT 기술의 의존도는 점점 많아지고, 이와 함께 축적되는 다양한 정보의 가치 및 활용은 미래에 반드시 필요한 자산으로 인식되고 있습니다.

그러나 이에 따른 역기능 또한 함께 커져가고 있습니다. 사이버 공간에서 자신도 모르게 유출되는 개인 정보, 악의적인 해커로 인한 금전적 손실, 사회 기반이 되는 공공 서비스에 대한 공격 등 사회 문제가 지속적으로 발생하고 있습니다. 이러한 문제들을 해결하지 않는 한 IT 기술의 미래는 결코 희망적일 수 없습니다. 특히 개인 정보와 관련된 프라이버시 문제는 일반 사용자들의 서비스 활용에 위축을 가져올 수 있어 새로운 서비스 창출을 불가능하게 할 수 있습니다. 프라이버시 문제를 해결하기 위한 연구는 수년전부터 미국, 유럽 등 선진국에서 다양한 프로젝트를 통하여 관련 기술을 개발하고 있습니다.

본 과제는 스마트 환경에서 사용자의 개인정보들이 안전하게 유통되기 위하여 인터넷 금융거래에 큰 위협이 되고 있는 피싱, 파밍 공격을 방지할 수 있는 기술, 공인인증서를 안전하게 사용하는 기술, 생활의 일부가 된 SNS 상에서 노출되는 프라이버시 분석 기술 들을 개발하며 이러한 결과물들은 인터넷 및 모바일 환경 서비스의 신뢰성을 향상 시켜 관련 사업 활성화 및 국가 경쟁력 강화에 기여할 것으로 확신합니다.

끝으로 연구개발 과제에 참여한 연구원 및 공동연구 기관 관계자 여러분들의 노고를 치하하는 바입니다. 앞으로 여러분 개개인의 열정으로 개발된 연구 결과물이 우리나라 정보통신 및 정보보호 기술 발전에 큰 기여가 있기를 기대합니다.

2015 년 12 월

한국전자통신연구원 원장 이 상 훈

제 출 문

본 연구보고서는 주요사업인 “시큐리티 큐레이션을 제공하는 프라이버시강화형 개인정보 유통보안 핵심기술 개발”의 결과로서, 본 과제에 참여한 아래의 연구팀이 작성한 것입니다.

2015 년 12 월

주관연구기관 : 한국전자통신연구원

연구책임자 : 책임연구원 진승헌

연구참여자 : 책임연구원 조현숙

책임연구원 김수형

책임연구원 조진만

책임연구원 조영섭

책임연구원 조상래

책임연구원 노종혁

책임연구원 최대선

선임연구원 김승현

선임연구원 김석현

공동연구기관 : (주)비씨카드

연구책임자 : 책임연구원 성기윤

연구참여자 : 책임연구원 이무연
책임연구원 정규식
책임연구원 김명석
책임연구원 오재민
선임연구원 심소정
선임연구원 김제성
선임연구원 최중휘

요 약 문

Ⅰ. 제 목

시큐리티 큐레이션을 제공하는 프라이버시강화형 개인정보 유통보안 핵심기술 개발

Ⅱ. 연구목적 및 중요성

가. 연구개발의 목적

○ 스마트 환경의 다양한 개체들로부터 안전하고 편리한 스마트 서비스를 제공받기 위해 리스크/협상에 기반한 시큐리티 큐레이션을 제공하는 프라이버시 강화형 개인정보 유통 보안 핵심 기술 개발

나. 연구개발의 중요성

○ 온오프라인 피싱, 개인정보 불법수집 등 스마트 환경에서 노출되기 쉬운 개인정보의 위험을 원천 차단하고 프라이버시가 보장되는 개인정보 유통 보안 기술 개발을 통해, 스마트 서비스 환경의 위험들로부터 사용자를 보호하고 단순 모바일 서비스를 개인정보 기반의 융·복합 고부가 서비스로 진화시킬 기술개발이 필요함

○ 스마트지갑 2.0은 온오프라인에서 지능화/개인화 서비스를 제공하기 위한 결제/개인정보기반 서비스 플랫폼 개념으로 발전하며, 이를 안전하게

구축하기 위해서는 온오프라인 위험으로부터 사용자를 보호할 프라이버시 프레임워크, 온오프라인 피싱 방지 기술, 개인정보 리스크 분석 기술과 같은 핵심기술 개발이 필요함

Ⅲ. 연구내용 및 범위

본 과제는 2013년부터 2015년까지 3년간 진행되었으며 주요 기술은 다음과 같다.

- ○ 개인정보 (ID, 인증정보, 결제정보) 유통 보안 인터랙션 기술
- ○ 온오프라인 피싱 방지 기술
- ○ 개인정보 리스크 분석 기술

연도별 내용 및 범위는 다음과 같다.

가. 1차년도(2013년) : 프라이버시 보호 모델 및 개인정보 유통 보안 요소기술 개발

- ○ 개인정보 (ID, 인증정보, 결제정보) 유통 보안 요소기술 개발
- ○ 스마트 환경의 프라이버시 보호 기반 기술 개발
- ○ 개인정보 공개 리스크 분석 기술 개발

나. 2차년도(2014년) : 연결/보안정책 기반 개인정보 유통 보안 시스템기술 개발

○ 개인정보 (ID, 인증정보, 결제정보) 유통 보안 시스템 기술 개발
○ 메모리해킹 피싱 공격 방지 기술 개발
○ 개인정보 연결 리스크 분석 기술 개발

다. 3차년도(2015년) : 추론/보안협상 기반 개인정보 유통 보안 응용기술 개발

○ 개인정보 (ID, 인증정보, 결제정보) 유통 보안 응용서비스 테스트베드 개발
○ 온오프라인 피싱/파밍 큐레이션 기술 개발
○ 개인정보 추론 리스크 분석 기술 개발

Ⅳ. 연구결과

본 과제의 수행을 통하여 확보된 주요 연구개발 결과는 아래와 같다.

○ 터치사인 시스템 개발
  • 오프라인 환경에서도 사용자가 소지한 휴대폰 또는 현금카드(스마트카드)로 안전하게 전자서명 가능한 NFC 기반 인증서 관리 및 이용 기술
○ 스마트채널3 개발
  • QR코드, 보안쿠키, OCR 기술을 이용하여 웹브라우저의 인증 절차를 스마트폰에서 대신 처리하는 서비스로, 상호인증 프로토콜과 보안토큰을 통해 서버/클라이언트가 안전하고 편리하게 인증하는 기능
○ 개인정보 공개 리스크 분석 기술 개발
  • SNS 등 프리 텍스트에 노출된 비정형적 개인정보를 추출하여 개인정

보의 소유자를 판단하고, 추출/분류된 개인정보에 대한 위험도를 판단하는 기술

○ 핸즈프리 결제 시스템

- 사용자가 상점 방문 시 비컨을 통해 구성된 체크인 Zone을 사용자 스마트폰이 인식하여 사용자 식별정보 노출 없는 안전한 체크인을 수행하는 핸즈프리 결제 시스템

○ 터치사인 - 온라인

- PC의 웹브라우저를 사용하여 웹서비스를 이용할 때 공인인증서를 이용한 전자서명 및 로그인 작업을 사용자 휴대폰에서 수행하는 기술

○ 개인정보 조합식별 위험 분석 기술

- 공공 데이터 등 집적 데이터 및 SNS/웹사이트 등의 단문 데이터에서 개인정보를 추출하고, 해당 개인정보의 주체를 식별하여, 주체별 개인정보를 연결/조합을 통해 위험도를 분석하는 기술

○ FIDO 인증 기술

- 바이오, 토큰, 패턴 등 다양한 방식의 사용자 인증 수단과 공개키 기반의 기기 인증을 결합한 인증 기술

○ 악성 BLE 비콘 탐지 기술

- BLE를 이용한 사용자의 결제/인증 서비스 시나리오에서 Relay Attack을 통해 공격자가 이득을 취하고 사용자가 피해를 볼 수 있는 부분에 대한 대응 수단으로서 악성 BLE 비콘 탐지 기술

○ 개인정보 큐레이션 시스템

- 스마트폰 앱이 사용자의 개인정보를 접근하는 시점에, 사용자에게 해당 접근 내역을 알리고, 사용자의 승인 내역에 따라 개인정보를 제공하는 실시간 개인정보 접근 제어 기능 개발

○ 개인정보 추론 리스크 분석 기술

- 파일 및 SNS, 웹 상의 다양한 공개 정보들을 조합, 연결하여 유의미한 개인정보를 추론할 수 있는 다양한 방법론을 적용하여, 비정형 개

인정보에 적합한 최적의 방법론을 찾고, 이 방법론을 적용하여 개인정보 추론 리스크를 분석

○ 개인정보 이상 접근 탐지 기술

- 기계학습, 사용자 패턴, 관리자 규칙 등을 이용하여 데이터베이스에 접근하는 이상행위를 탐지하여 개인정보를 보호하는 기술

○ 논문

- SCI(E) 논문 4건 게재
- 국내외 논문 26건 게재

○ 특허

- 국제 특허 5건 출원, 1건 출원 중
- 국내 특허 16건 출원, 1건 출원 중

○ 표준화

- 국제 표준 기고서 3건 채택
- 국내 표준안 11건 채택

○ 기술이전

- 기술이전 24건 완료

Ⅳ. 연구개발결과의 활용계획

본 과제의 연구개발 결과의 활용계획은 아래와 같다.

○ FIDO 인증 기술은 사용자의 다양한 생체정보를 이용하여 전자결제 서비스의 사용자 간편 인증 솔루션으로 활용이 전망됨

○ 악성 BLE 비콘 탐지 기술은 지불, 결제, 출입통제 관련 업체의 BLE 비콘 기반 오프라인 간편 인증 솔루션에 대한 보안취약성을 개선할 수 있음

○ 개인정보 큐레이션 시스템은 악성코드가 숨겨진 앱의 프라이버시 침해를 실시간으로 차단하는 서비스에 활용

○ 개인정보 추론 리스크 분석 기술은 개인정보 추론을 통해 민감정보가 아닌 일반 정보들을 기존 개인정보와 연계하여 개인의 민감정보를 도출할 수 있음을 확인한 것으로 다양한 영역에서 추론 기법이 확대 적용될 수 있음

○ 개인정보 이상 접근 탐지 기술은 데이터베이스 이상행위 탐지 및 FDS 기술에 활용될 수 있음

Ⅴ. 기대성과 및 건의

가. 기술적 측면

○ 관계망(SNS)/스마트환경에 노출된 개인정보를 분석하여 위험을 평가하는 기술은 스마트지갑의 원천 보안기술로 활용 기대

○ 스마트환경에서의 프라이버시 보호 및 개인정보 유통을 위한 보안 핵심 원천 기술과 지재권 확보

○ 시큐리티 큐레이션과 개인정보 유통 보안 기술 개발을 통해 관련 모바일 서비스 기술 분야에서 세계 수준의 기술경쟁력 확보 가능

나. 경제 산업적 측면

○ 개인정보 관리 분야의 시장규모는 2015년 세계 63.5조, 국내 1.2조원으로 예상되며, 세계시장 점유율 1% 확보 시 6천 3백억 원의 시장개척 가능

○ 프라이버시 우려로 침체되었던 관련 서비스 산업의 높은 성장과 고용을 촉진함

- 핵심기술에 대한 중요 특허를 선점하고 기술 보급하여 국내 산업경쟁력 강화
- 스마트 의료·헬스/금융/정부 등 사용자의 민감한 정보를 다루는 공공분야에서 뿐만 아니라, 정보수집 어려움으로 위치정보만을 사용하는 수준의 광고, 추천 등의 모바일 서비스를 고도화하기 위한 기반기술로 활용될 것임

다. 사회적 측면

- 온오프라인 피싱/사기, 개인정보 유출 등의 범죄 피해를 경감시킴
- 온라인과 오프라인 환경에서 사용자 스스로 자기결정권을 가지고 정보를 공유 · 제어할 공통 기술로 활용 예상
- 인증정보의 유출 및 오남용에 취약한 지식기반 인증(예: 패스워드) 기술을 대체하여 생체기반 인증, 소지기반 인증 기술을 제공해 보안성과 편의성이 강화된 전자금융 서비스 활성화 기대

ABSTRACT

Ⅰ. TITLE

Development of core technology in privacy enhanced personal information distribution security for providing security curation

Ⅱ. THE OBJECTIVE AND IMPORTANCE

A. Objective

Development of core technology in privacy enhanced personal information distribution security for providing security curation based on risk and negotiation to receive secure and convenient smart service from various entities of smart environment

B. Importance

○ It is necessary to develop a technology to convert a simple mobile service into a personal information based converged and high value-added service and prevent danger of personal information easily exposed at smart environment where there are securty incidents such as online and offline phising, illegal collection of personal information, etc.

○ It is also necessary to develop core technologies such as privacy framework that protects user from security risk existing in online and offline, prevention of online and offline phising and analysis of the risk of personal information. These technologies enables to deploy secure payment and personal information based the service platform to provide intelligent and personalized service in online and offline in Smart Wallet 2.0

Ⅲ. THE CONTENTS AND SCOPE OF THE STUDY

This project is carried out for three years from 2013 to 2015. The main technologies are as follows.

○ Personal information (ID, Authentication information, Payment information) distribution security interaction technology
○ Online and offline phising prevention technology
○ Personal information risk analysis technology

Contents and scope of the project in each year are listed as follows.

A. 1st Year (2013) : Development of privacy protection model and personal information distribution security core technology

- Development of personal information (ID, Authentication information, Payment information) distribution security core technology
- Development of privacy protection technology in smart environment
- Development of personal information open risk analysis technology

B. 2nd Year (2014) : Development of connection and security policy based personal information distribution security system

- Development of personal information (ID, Authentication information, Payment information) distribution security system technology
- Development of memory hacking attack prevention technology
- Development of personal information connection risk analysis technology

C. 3rd Year (2015) : Development of inference and security negotiation based personal information distribution security application technology

- Development of personal information (ID, Authentication

information, Payment information) distribution security application testbed

- ○ Development of online and offline phising and pharming curation technology
- ○ Development of personal information inference risk analysis technology

Ⅳ. RESULTS

The main outcome produced by performing the project are as follows.

- ○ Development of TouchSign system
- ○ Development of Smart Channel 3
- ○ Development of personal information open risk analysis technology
- ○ Development of HandsFree payment system
- ○ Development of TouchSign Online
- ○ Development of Personal information combined identification risk analysis
- ○ Development of FIDO authentication
- ○ Development of malicious BLE beacon detection
- ○ Development of Personal Information curation
- ○ Development of Personal information inference risk analysis
- ○ Development of personal information anomaly access detection
- ○ Papers
  - SCI(E) – 4 published

- Non SCI(E) – 26 published

○ Patents

- International – 5 patented and 1 proceeding
- Domestic – 16 patented and 1 proceeding

○ Standard

- International contribution – 3 accepted
- Domestic standard – 11 approved

Ⅴ. EXPECTED RESULT & PROPOSITION

A. Technical Aspect

○ The technology estimating a risk by analyzing disclosed personal information in SNS and smart environment is expected to use it as a core security technology of Smart Wallet

○ Obtaining intellectual patents and core technologies for privacy protection and personal information distribution in smart environment

○ It is possible to have world best technological competitive advantage in mobile service area by developing security curation and personal information distribution security technology, which is an unexplored field.

B. Economical and Industrial Aspect

○ It is possible to open a new market in personal information field,

which its market is forecasted to be 63.5 trillion worldwide and 1.2 trillion won in Korea. This would be 630 billion won if a market share of this technology reached to 1%.

- It can promote an employment and high growth in service industry which experienced economic downturn because of privacy fear
- Reinforcing domestic industry competitiveness by providing developed technologies and securing core patents regarding core technologies
- It is possible to be used in two areas. The one is public sector where manages sensitive personal information such as smart medical care and health, finance and government. The other is private sector where there is strong requirement to provide more advanced intelligent and personalized services

C. Social aspect

- It is expected to decrease criminal damage that includes online and offline phising and fraud and disclosure of personal information
- It can be expected that developed technologies can be utilized in every online and offline service and industry that needs to use personal information since the procedure to obtain a consent for the usage of personal information is much simplified
- The technologies can also be used for basic technology to control and share personal information when a user wish to do with his own control in online and offline environment

CONTENTS

List of Tables

List of Figures

목 차

표 목 차

그 림 목 차

제 1 장 서 론

제 1 장 서 론

제 1 절 개발기술의 중요성 및 필요성

1. 개발 대상 기술의 개요

○ 스마트 환경의 다양한 개체들로부터 안전하고 편리한 스마트 서비스를 제공받기 위해 리스크/협상에 기반한 시큐리티 큐레이션을 제공하는 프라이버시 강화형 개인정보 유통 보안 핵심 기술 개발

○ 주요 기술

- 개인정보 (ID, 인증정보, 결제정보) 유통 보안 인터랙션 기술
- 온오프라인 피싱 방지 기술
- 개인정보 리스크 분석 기술

[그림 1-1] 기술 개발 개념도

○ 적용 서비스

- 스마트 의료·헬스/금융/정부 등 사용자의 민감한 정보를 다루는 공공분야에서 개인정보보호를 위한 기반 기술로 적용
- ATM, POS, 스마트패드, 사이니지 등 오프라인 환경의 스마트단말을 통한 결제, 인증, 개인정보 공유를 위한 핵심 기술로 활용
- 사이트 로그인, 온라인 뱅킹, 모바일 본인인증 등 간편하고 보안이 강화된 사용자 인증을 요구하는 포탈, 금융, 통신 서비스 분야

2. 개발 대상 기술의 중요성

가. 개발 대상 기술의 필요성

○ 최근 인터넷 피싱·사기, 개인정보 노출로 인한 프라이버시 침해 등 IT고도화 시대의 역기능·부작용으로 인한 개인피해가 증가하는 추세임

○ 또한, 오프라인 환경에서도 점차 높은 프로세싱 파워와 항시 연결된 네트워크를 가진 스마트기기들이 보급되고 있어 이를 통한 오프라인 개인정보 불법수집, 피싱 등 피해도 발생하고 있음

○ 한편, 구글, 애플, 마이크로소프트, 비자카드 등 업체들은 전자지갑 사업을 추진하고 있으나, '빅브라더 우려'로 인해 서비스 확산에 어려움을 겪고 있으며, 최근 글로벌 IT기업들의 개인정보 불법수집과 악용으로 개인정보 활용에 대한 프라이버시 이슈와 사용자의 부정적 인식이 스마트 서비스 산업의 발전과 활성화에 심각한 장애요소가 되고 있음

○ 또한, 사용자 스스로 개인정보를 보호하고 활용할 수 있는 권리에 대한 요구가 높아지고 있어 이를 체계적으로 지원할 기술 개발이 시급함

[그림 1-2] 기술의 필요성

○ 이에, 온오프라인 피싱, 개인정보 불법수집 등 스마트 환경에서 노출되기 쉬운 개인정보의 위험을 원천 차단하고 프라이버시가 보장되는 개인정보 유통 보안 기술 개발을 통해, 스마트 서비스 환경의 위험들로부터 사용자를 보호하고 단순 모바일 서비스를 개인정보 기반의 융·복합 고부가 서비스로 진화시킬 기술 개발이 필요함

나. 연구개발과제의 중요성

○ 스마트지갑 2.0은 온오프라인에서 지능화/개인화 서비스를 제공하기 위한 결제/개인정보기반 서비스 플랫폼 개념으로 발전하며, 이를 안전하게 구축하기 위해서는 온오프라인 위험으로부터 사용자를 보호할 프라이버시 프레임워크, 온오프라인 피싱 방지 기술, 개인정보 리스크 분석 기술과 같은 핵심기술 개발이 필요함

[그림 1-3] 기술의 중요성

○ ‘개인화’, ‘추천’, ‘맞춤’으로 대변되는 개인정보기반 서비스들은 최근 모바일 플랫폼의 발전과 더불어 급증 추세였으나, 개인정보 확보 문제로 서비스 확산에 어려움이 있으며, 구글, 페이스북 등 IT기업들은 무리하게 개인정보를 수집하여 여러 가지 사회 문제가 되고 있음

○ 프라이버시가 보장된 개인정보 유통 보안 기술은 스마트 쇼핑/광고/정부 등 개인정보필요 서비스에서의 개인정보침해·오남용 등 부작용을 해소하여 이용자중심 고부가 서비스로 진화하기 위해 반드시 필요한 기술임

제 2 절 국내외 관련 기술의 현황

1. 국내외 기술 및 표준화 현황

가. 국내 기술 동향 및 수준

○ 국내 모바일 결제 서비스는 국내 통신사를 주도로 금융사, 제조사, 유통사 마다 특화된 전자지갑 서비스를 제공함

- 통신사는 SK텔레콤 ‘스마트월렛’, KT ‘모카 페이’, LG유플러스 ‘스마트월렛’을 출시함
- 금융사는 카드사를 중심으로 통합 전자지갑 서비스를 제공하려는 움직임이 있음
- 유통사는 신세계 ‘S캐시’, 롯데 ‘캐시비’, GS+ 티머니 ‘팝티머니’ 등 다양한 전자지갑을 선보임
- 제조사는 삼성전자 ‘삼성월렛’을 출시함

○ 통신사, 플랫폼 서비스 및 PG사 들이 서로 경쟁적으로 모바일 결제 서비스를 출시하며 극심한 경쟁을 하고 있음

- 다음카카오는 LG CNS와 협력하여 개정된 전자상거래 규격에 맞춰 카카오페이라는 결제 플랫폼을 출시함
- LG유플러스는 가상카드번호를 사용하는 페이나우 서비스를 출시했으며, SKT는 신용카드사, 은행 등과 제휴해 스마트월렛 서비스와 결합하여 페이핀을 준비했으며 KT도 모카페이를 모카월렛과 결합하여 서비스를 제공중임
- PG사 중 KG이니시스는 원클릭 간편결제 서비스인 “케이페이”를, KCP는 NFC기반의 “셀프페이”의 개발을 완료하여 서비스를 제공 중임

○ NFC 인프라 부족 문제로 인해 비 NFC기반 모바일 결제서비스가 다수 등장함

- 모바일 결제 시장에서 대표적인 기술인 NFC에 대한 인프라 구축 문제와 개인정보 유출 등으로 확산속도가 더디어 지고 있으며, 최근 앱기반 및 바코드/QR코드 기반의 비NFC 기반의 모바일 결제 서비스가 등장함
- 바이오 인식 기술을 적용한 모바일 지급 결제 및 사용자 인증을 위해서 모바일 바이오정보 탑재기술이 연구 중에 있음
- 다날, 바코드결제 솔루션 바통(BarTong)에 크루셜텍의 지문인식 기술을 도입한 바통 지문인식 서비스를 팬택의 스마트폰 '베가 LTE-A'에 적용됨
- 이니텍의 안드로이드 OS 기반 일체형 'SE POS' 는 자사의 보안솔루션을 적용한 카드리더기(MSR) 보안 기능을 일체화함

○ 액티브X를 탈피한 공인인증서 사용 기술과 대체인증 기술에 대한 연구가 활발함

- ETRI는 보안성이 취약한 패스워드 대신 지문, 얼굴 등 생체인식과 스마트폰 잠금해제 패턴, H/W 칩 등 강력한 인증 수단을 사용할 수 있는 FIDO Alliance의 UAF(Universal Authentication Framework) 기술을 개발함
- KISA는 최신 OS 윈도8 기반의 모바일 플랫폼에 알맞은 공인인증서 처리를 위해 라온시큐어의 윈도8 터치스크린용 '윈도공인인증서관리' 앱을 개발함
- 시큐에프엔은 생체정보인식 기반의 전자서명 방법 및 생체정보인식 기반으로 전자서명된 전자문서를 검증하기 위한 솔루션인 '아이디트러스트'를 개발함
- 크루셜텍은 전자금융거래 보안인증 수단으로 터치스크린과 지문인식 센서가 일체화되는 '언더글래스 BTP' 연구 중에 있음
- 일부 갤럭시 넥서스에서 얼굴인식스캐너 구현 등 모바일 바이오인식에 통신사업자, 스마트폰 제조업체에서 장기적 투자가 예상됨

○ 메모리 해킹 공격을 막기 위한 다양한 솔루션이 개발되고 있음

- 큐브피아 '권가 금융해킹방지솔루션', 이니텍 '이니세이프샌드박스', 시큐브 '스마트 그리핀', 카스퍼스키랩 '카스퍼스키 프러드 프리밴션', 소프트포럼 '제큐어투웨이', 마크애니 '이뱅킹세이퍼', 잉카인터넷 '엔프로텍트 X 가드' 등의 솔루션이 존재함
- 거래 연동 OTP, 추가 인증 시스템, 이상 징후 탐지 시스템, 입금계좌 지정제 개선 등 금융 서비스의 메모리 해킹을 포함한 신종 피싱 공격에 대응하는 인증 강화 솔루션이 활발하게 적용됨
- JB 전북은행은 2014년 10월, 스마트폰에 IC카드 접촉하여 인터넷뱅킹, 공인인증서 발급을 수행하여 보이스 피싱, 메모리해킹을 방지하는 '세이프터치' 인증서비스 시작
- 경찰청은 호스트파일의 감염된 사이트 내용을 수정하여 파밍방지를 제공하는 '파밍캅'을 개발하여 무료로 배포중임
- 케이사인은 2014년 5월, 스마트폰을 이용해 이중 인증과 피싱 방지 기능을 제공하는 '위즈사인2'를 출시함
- 소프트포럼은 2014년 4월, '2채널 기반의 사용자 인증 장치 및 방법' 특허 출원으로 스마트폰을 통해 암복호화 인증을 수행하여 메모리변조, 중간자 공격 등을 무력화하는 방안을 제시함

○ 빅데이터 기술을 이용한 보안 강화 방안이 요구되고 있으며, 빅데이터에서 사용자 프라이버시를 보호하는 방안들이 연구되고 있음

- 안행부는 '공공데이터의 제공 및 이용 활성화에 관한 법률'과 동법 시행령·시행규칙을 2013년 10월 31일부터 시행하고, 2017년까지 단계적으로 9,470종에 대한 공공데이터를 개방하기로 함. 개방되는 공공데이터에는 기본적으로 정형 개인정보가 노출되지 않도록 가이드 하고 있으나, 다양한 비정형 개인정보 및 조합/추론을 통한 민감정보 노출은 차단이 어려움
- 방통위는 2014년 11월 12일 '온라인 개인정보 취급 가이드라인'을 발표

함. 서비스와 무관한 개인정보 수집 및 포괄적 동의 등 기존 관행에 제동, 또한 개인정보 보유기간 명확화를 추진함

- 이스트소프트는 PC 내에 주민등록번호, 계좌번호, 신용카드번호 등 총 7가지의 민감한 개인정보가 담긴 문서를 검색/암호화/삭제 할 수 있는 '알키퍼 1.0'을 출시함
- 인포섹은 구글 개인정보조사서비스 GPISS(Google Personal Information Survey Service)를 출시하여, 특정 URL에서 노출되어 있는 개인정보 조사 및 특정 개인정보의 노출 여부를 분석함
- 2014년 7월, 단순히 주민번호, 이름, 전화번호로 구글 검색을 통해 해당 정보가 포함된 다양한 문서를 찾을 수 있어 개인정보 유출 우려가 제기됨

나. 국외 기술 동향 및 수준

○ NFC/비 NFC 기반의 모바일 결제서비스 기술이 활발하게 개발 중임

- NFC 기반의 모바일 결제 서비스로 중국 은련(China union pay)은 금융 microSD 카드를 결제수단으로 사용하고 있고, 미국이나 호주의 경우에도 금융 microSD를 이용한 모바일 결제 서비스를 준비 중에 있음
- 비 NFC 기반의 대표적인 주자인 미국의 Square사의 결제시스템은 2010년 카드 판독기 결제 방식에서 시작하여 2012년에는 앱결제 방식(Pay with Square)를 출시함
- 바이트라이트는 NFC와 흡사한 'LFC(Light Field Communication)'라는 통신 방식을 활용하여 대금 지불 시스템 개발 중에 있음
- 페이팔은 2013년 9월 USB 드라이브와 같은 모습에 전원 아답터와 결합된 형태의 비콘(Beacon) 기술을 이용한 블루투스 모바일 결제 서비스를 제공함
- 에스티모테(Estimote)는 아이비콘(i-Beacon) 지원 장치를 공개했고, 2013년 10월 초에는 미국 메이저리스의 뉴욕 메츠 홈구장인 시트 필드

가 아이비콘 시범 서비스를 시작함

- 애플은 최근 NFC와 지문인식 기술에 보안칩을 이용하여 사용자의 지문 정보와 카드정보를 관리하는 스마트카드 기반의 결제시스템인 애플페이를 출시하여 미국에서는 빠르게 사용자를 확보하고 있는 상황임

○ 인증기술이 비밀번호 방식에서 생체인식, 보안토큰, 뇌파인식 등으로 급속하게 발전하고 있음

- 구글은 2015년부터 각종 웹사이트에 직접 ID, 비밀번호를 입력하는 대신, 보안성을 높이기 위해서 별도 USB 장치를 이용한 '유니버셜 세컨드 팩터(U2F)를 채택함
- UC버클리 대학의 댄 와그너(Dan Wagner) 교수는 웨어러블 방식의 보인인증 단말기가 보안 업체의 차세대 화두라고 주장함
- 세계적인 터치 기술 기업 시냅틱스가 지문인식 업체인 밸리디티를 2억5천500만 달러에 인수하여 터치스크린에 지문인식 센서가 탑재될 것으로 예상됨
- 캐나다의 바이오님(Bionym)은 심장 박동을 인증 수단으로 사용하는 웨어러블 스마트 키 '나이미(Nymi)' 개발
- 모바일 보안 업체 패스밴(PassBan)은 생체 인식 기반의 보안 애플리케이션 '패스보드(Passboard)'를 공개. 패스보드는 음성은 물론 안면 인식, 장소 인식, 동작 인식 등을 이용해서 사용자를 인증하는 것이 가능함
- 모토로라는 전자문신과 알약 형태의 비밀번호를 개발하며, 장기적으로 전자 칩이 들어간 알약을 삼켜 비밀번호를 대체하는 프로젝트도 진행 중임
- 픽셀핀(PixelPin)은 저장된 배우자의 사진에서 사전에 설정된 방식으로 사진의 네곳을 클릭하면 로그인이 되는 사진 인증방식을 개발함
- FIDO Alliance는 지문, 얼굴 등 생체인식과 스마트폰 잠금해제 패턴, H/W 칩 등 강력한 인증 수단을 사용할 수 있는 인증장치를 기반으로 하

는 개방형 인증 프레임워크인 UAF 표준을 발표하여 모바일 환경에서 사용자 인증 및 전자서명을 제공하는 기술을 발표함

○ 온라인 피싱은 갈수록 고도화되고 단시간에 이루어지기 때문에, 다양한 피싱 공격에 대한 실시간 대응이 요구됨

- 美 파이어아이는 2013년 11월 스피어 피싱 등 지능화된 이메일 피싱 공격에 대응하기 위해서 자사의 가상화 엔진을 적용한 '파이어아이 이메일 위협 방어' 플랫폼을 공개함
- 안티피싱워킹그룹에 따르면, 2012년 상반기에 9만 3천여 건의 unique 공격이 6만 4천여 domain을 대상으로 이루어졌으며, 피싱사이트의 구동 시간은 평균 6시간에 못 미침. 또한 공유 가상 서버, 단축URL을 이용한 형태에 피싱이 특징이었음
- 브라우저의 제로데이 취약점을 이용하여 특정 사이트에 방문하는 사용자를 악성코드에 감염시키고, 금융정보를 탈취하는 Man-In-The-Browser 공격이 활성화됨
- 시만텍에 따르면, 미국 정부 웹 사이트로 가도록 되어 있는 일부 단축 URL 링크를 훔쳐서 피싱사이트로 유도하는 공격이 발견되었으며, 15%의 클릭이 스팸 웹사이트로 유도됨
- 2010년부터 MITM 공격을 피싱에 활용한 액티브 피싱 공격이 실제로 등장하였으며, 기존 피싱 공격의 해결책으로 여겨졌던 2채널 인증 솔루션에 대해서도 취약점이 드러남
- 인포섹은 한국EMC와 제휴를 통해 인터넷 사기거래 위협에 대응하고 개인정보 유출을 선제적으로 대응하는 보안관제서비스를 운영하여 피싱 방지, 악성 코드 방지 등의 기능을 제공함

○ 빅데이터 기술을 이용하여 보안에 활용하는 방안이 다수 제안되었음

- NSA의 도청으로 인해 고객 전화 통화나 문자메시지, 이메일 등을 암호화해 외부 추적을 차단하는 서비스를 제공하는 '사일런트 서클(Silent Circle)'이 호황을 누리고 있음
- NEC는 빅데이터를 이용한 분석 클라우드 서비스의 하나로 얼굴 인증 기술을 활용하여 카메라 영상에서 실시간으로 인물을 검색하고 자동으로 특징을 데이터베이스에 등록, 수상한 사람을 검색하는 서비스를 발표하였음
- 트룰리오의 프로필 플러스라는 서비스는 스팸용 가짜 Facebook 계정을 식별하여 광고비용에서 배재하는 기술인 필터링 서비스를 제공함
- EMC RSA는 전체 네트워크 이상 징후로부터 로그 데이터 분석 등 지속적인 인프라 모니터링을 통한 침입여부 파악에 빅데이터가 필수적이라고 발표함
- 맥아피는 보안취약점 관련 데이터, 해결방법 등을 저장한 글로벌쓰렛인텔리전스(GTI)와 함께 방대한 로그데이터를 기존보다 2~3배 빠르게 처리하는 '나이트로'라는 빅데이터 솔루션을 접목하였음
- 시만텍은 자사가 보유하고 있는 인터넷 보안위협 데이터 수집 시스템 '글로벌 인텔리전스 네트워크'를 활용해 매일 80억 개가 넘는 보안위협을 분석하고 13억 개 시스템을 통해 악성코드를 수집하였음
- 인덱세우스(Indexeus)라는 자신의 이름만 입력하면 해킹 등을 통해 유출된 ID, 비밀번호, 이메일 등 정보를 알려주는 검색 서비스도 등장함

○ 빅데이터 사용을 활성화하기 위해서 사용자들의 프라이버시를 강화하는 법안들이 발의되었고, 사용자가 본인의 데이터를 빅데이터에서 조회/관리할 수 있게 도와주는 서비스가 등장함

- 영국 개인정보 보호 관련 시민단체인 '빅브라더워치(Big Brother Watch, BBW)는 최근 실시한 조사에서 EU를 비롯한 다수의 국가들이 대기업의 개인정보 수집 및 온라인에서의 사생활 침해에 대해 높은 우려를 나타낸

것으로 밝힘

- 위스콘신(Wisconsin) 주의원은 2013년 4월, 고용주 등이 구직자 등에게 개인의 소셜미디어 정보 요구를 금지하는 '소셜미디어 개인정보보호법' 입법을 추진함
- 영국의 정보감독위원회가 발의한 `데이터보호규약(Code of practice for data protection)`에 따라 인터넷 상에서 돌아다니는 개인정보 등을 식별할 수 없는 특정 형태로 변환하는 데이터 익명화를 법적으로 명시할 수 있게 되었음
- 독일 법원은 구글의 '스트리트뷰(Street View)' 서비스 구현을 위한 개인정보 수집은 개인정보보호법을 위한 행위라고 판결하고 14만 5,000유로(약 2억 1,00만원)의 벌금을 부과함
- EU가 발표한 개인정보 보호지침 개정안에는 자동처리기술에 의한 프로파일링과 예측서비스를 제한하고 개인정보 사용에 대한 사용자의 명시적 동의를 의무화하도록 규정하고 있음
- 미국 데이터 브로커(중개업자) 액시온(Acxion)은 소비자가 직접 자신의 개인정보 수집과 활용 현황을 확인하는 사이트 '어바웃더데이터닷컴(AboutTheData.com)' 운영을 시작함
- 미국 개인정보 수집 파문 이후, 이용자 스스로 온라인상에 존재하는 본인의 사진이나 메시지를 삭제할 수 있는 애플리케이션 '위커(Wickr)' 내려받기 건수가 156% 증가함
- 미국 ReputationDefender는 개인의 온라인 활동 감시와 특정 웹사이트에 저장된 개인정보 삭제 서비스를 제공함
- Google `미 온더 웹`(Me on the Web)은 사용자 본인의 관련 검색어를 입력하여 웹상에 알려진 자신의 평판을 감시하는 기능을 제공함
- 유럽의 Allow는 회원의 개인정보 판매를 대행하는 서비스로, 고객의 개인 관심사에 맞춘 광고를 보여주기 전에 허가를 요청하며, 마케팅 업체들로부터 고객의 개인정보를 제거하는 방식으로 개인정보의 가치를 높임

○ 핀테크가 핫이슈로 떠오르는 가운데, 새로운 유형의 금융, 지불 방법에 대한 보안 제공이 관건이 되고 있음

- 애플 페이의 출시로 NFC 결제(3세대)가 이슈화되고 있어, 차세대 결제 기술인 BLE 기반 결제(4세대) 및 보안 기술 개발이 시도되고 있음
- 전통적 전자금융은 물론, 핀테크에서도 피싱/파밍, 메모리해킹은 보안 대책이 반드시 필요한 중요한 이슈임. 그러나, 주로 스타트업 등 보안 기술에 익숙하지 않는 핀테크 사업자의 특성상 필요한 보안 대책을 모두 구비하기에는 한계가 있어, 이를 해결하는 기술이 적용될 수 있음
- 다양한 유형의 핀테크 서비스 구조를 통해 유통되는 개인정보가 유출되고 악용될 가능성이 증가함. 따라서 개인정보 유통상 프라이버시 보호 기술의 적용성이 높음

다. 국내외 표준화 동향

○ 인증/결제

- TTA는 2008년 X.509 인증서를 이용한 가명 기반의 익명인증 기술 표준화를 추진하여 국내 표준으로 제정하였고, 2010년 그룹 서명 기반의 프라이버시 강화형 익명인증인가기술에 대한 국내 표준을 제정하였음
- TTA PG502에서 모바일 ID 관리 기술 및 모바일 지불 기술 관련하여 2010년부터 국내 표준을 추진하여 기술의 상호호환성 및 활용성을 높이고 있음
- 지식경제부 기술표준원은 2012년 ETRI와 비씨카드가 개발한 '차세대모바일카드'를 스마트폰 결제 서비스를 위한 모바일 지급결제의 국가표준으로 제정하였음
- ITU-T 정보보호 연구반(SG 17)은 2012년 9월 회의에서 '모바일 디바이스를 이용한 다중 인증 메커니즘'에 관한 표준화를 우리나라 주도로 추진

하여, 다양한 인증 메커니즘들을 복합적(ID/패스워드+ 공인인증서, ID/패스워드+ 보안토큰, ID/패스워드/바이오토큰 등)으로 결합 구현하기 위한 효율적인 다중 인증 메커니즘 표준을 개발 중임

- OASIS는 보안 Assertion기반의 SAML 표준을 개발하였고, ITU-T는 ID 관리 과정에서 요구되는 객체 인증 및 보증을 위한 프레임워크와 인증에 영향을 미칠 수 있는 요소들의 기준, 위협 등을 정의한 'Entity Authentication and Assurance' 표준을 개발 중이며, ISO는 ETRI에서 제안한 익명인증 기술에 대한 표준화를 완료하였음
- FIDO Alliance에서는 개방형 세컨드 인증장치 표준인 U2F와 개방형 인증 프레임워크인 UAF 표준에 대한 초안 검토를 마치고 2015년 12월에 공식 표준으로 승인하였으며 현재는 U2F와 UAF를 통합하는 FIDO 2.0 기술규격을 개발 중에 있음

○ 안티 피싱/파밍

- TTA는 2006년 악성코드 정의 및 대응방법이 포함된 악성코드 감염 예방을 위한 가이드를 제정하였으며, 2010년 악성코드 감염예방을 위한 지침을 제정하였음
- TTA는 2009년 HTTP를 위한 상호 인증 프로토콜을 표준화하여 간단한 패스워드기반의 인증 방식을 사용해 HTTP 서버와 클라이언트간의 상호 인증을 제공하는 프로토콜에 대한 기술 규격을 정의하였고, 2012년에는 피싱 사고에 대한 대응 지침을 표준화하여 피싱 방지를 위한 보안 기술 장치 및 보안 방법을 이용한 보안 지침을 정의했음
- ITU-T는 2011년에 ICT 네트워크에서 악성코드 감염 예방을 위한 가이드라인 표준을 제정(X.1205)했으며, 2012년 ITU-T 악성코드의 속성 및 분류체계에 대한 표준화 작업을 진행(X.maec)했음
- 2012년 Google, Facebook, 마이크로소프트(MS), 야후 등 주요 기업들이 이메일 피싱과의 전쟁을 선포하고 피해 방지를 위한 시스템 표준을 만

들기 위해 ‘DMARC’ 조직을 구성하였고, 현재 표준화 세부사항에 대해 국제인터넷기술위원회(IETF)에 제출할 계획임

- 금융위원회는 2014년 8월 ‘전기통신금융사기 방지대책협의회’를 개최하여 스마트폰에 스미싱을 기본 차단하는 앱을 탑재하기로 결정하였음
- IETF는 HTTP 레벨에서의 피싱 방지를 위하여 2012년 11월에 TLS Channel Id, 2014년 10월에 HOBA(HTTP Origin-Bound Authentication) 표준화를 진행 중임

○ 빅데이터/SNS 프라이버시

- TTA는 2009년 TC5 PG502에서 자기제어 강화형 디지털 아이덴터티 공유 프로토콜을 표준화하여 사용자가 자신의 개인정보를 공유함에 있어 사용자 중심에서 사용자가 모든 통제권을 가지고 아이덴터티 공유 및 동기화를 할 수 있는 프로토콜을 정의함
- ITU-T SG17은 사용자 프라이버시를 강화한 사용자 중심의 아이덴터티 공유 프레임워크를 2009년에 X.1251 - A framework for user control of digital identity 표준으로 제정함
- TTA는 2011년 모바일 아이덴티티 관리 프레임워크를 표준화하여 모바일 단말에서 사용되는 모든 아이덴티티의 보안 및 프라이버시 보호, 모바일 아이덴티티의 안전하고 편리한 사용, 서비스 상호 연동, 모바일 아이덴티티에 기반에 고부가 서비스 개발을 제공하는 퍼스널 모바일 아이덴티티 관리 프레임워크를 정의하였음
- 방송통신위원회와 한국인터넷진흥원은 2012년 빅데이터 환경에서 높아진 개인정보보호 위험에 선제적으로 대응하기 위해 ‘개인정보보호 법제정비 연구 포럼’ 내 빅데이터 연구반을 구성함
- 행정안전부는 2011년 5월 ‘공공기관 홈페이지 개인정보 노출방지 가이드라인’을 배포하여 검색엔진 등 빅데이터에서 사용자 프라이버시를 노출시키지 않는 다양한 방법을 제시함

- ISO/IEC JTC1과 ITU-T는 SC 27(Security techniques)에서 빅데이터 기반의 사생활 보호 및 개인정보 보호 측면에서의 표준화를 추진하고 있음. 2013년 11월 ISO/IEC JTC1 차원에서 SG(Study Group)을 발족하여, 표준화를 위한 준비 작업을 진행하고 있음
- W3C는 2012년 4월 BigData Community Group을 운영하여 빅데이터 처리를 위한 표준 구조, 프로그램 API 정의, 상호 호환성, 보안, 저비용을 보장할 프로그램 언어 개발 등을 진행하고 있음
- 미국 NIST는 2013년 6월 Vendor 독립적인 Big Data 표준화를 위해 NBD-PWG(NIST Big Data - Public Working Group)을 발족함. 5개 Subgroup을 운영하며, 2014년 10월 IEEE와 연계하여 워크숍을 개최함. 해당 위크숍에서 관련 규격을 발표함

2. 국내외 시장 현황

가. 국내외 시장 규모 및 수출입 현황

나. 국내외 주요 수요처 현황

[표 1-1] 국내외 주요 수요처 현황

수요처	국명	수요량	관련제품
금융/전자정부	세계	30억개[1]	인증 솔루션
금융	세계	4억 2350만개[2]	안티 피싱 솔루션
SNS 사이트	세계	17.9억개[3]	프라이버시 분석 툴

다. 핀테크 현황과 보안 기술

○ 핀테크[4] 현황

- 세계 모바일 결제시장은 2017년 7,210억 달러 규모로 연평균 25.2% 성장할 것으로 전망됨[5]
- 국내 모바일 결제시장 규모도 2014년 2분기 3조 1,930억원으로 전년 동기(1조 3,480억원) 대비 약 2.4배 성장
- 지난 5년간 핀테크 기업에 대한 투자 규모는 전 세계적으로 3배 이상 성장(2008년 9.2억 달러 -> 2013년 29.7억 달러)[6]
- 정부의 결제 간편화 정책(공인인증서 의무사용 폐지(5.20), 전자상거래 결제 간편화 방안 발표(7.28), 신용카드 가맹점 표준약관 개정(8.28) 등) 으로 2014년 11월 9개 PG사가 간편결제서비스를 출시하였거나 출시할 예정임
- 애플은 지문인증을 통한 근거리무선통신(NFC) 결제서비스 애플 페이'를 2014년 10월 전자지갑에 탑재

---

1) ITU, "ICT facts and figures – The World in 2014, 2014.4
2) comScore, Inc, "1 in 4 Internet Users Access Banking Sites Globally", 2012.6.15
3) statista, 'Number of socal network users worldwide', 2014.11
4) 핀테크(FinTech) :IT 신기술을 활용한 신종 금융서비스를 의미하며, 해외송금, 지급결제, 개인자산관리, 크라우드 펀딩 등에 적용
5) Gartner, "Forecast: Mobile Payment, Worldwide, 2013 Update", 2013.6.4
6) Accenture, "The Boom in Global Fintech Investment", 2014.4

- 월마트, 베스트바이 등 미국 14개 주요 대형 유통업체는 코드 스캔(비NFC) 방식의 자체 결제서비스를 2014년 9월 출시하였음
- 국내는 2010년 SKT의 전자지갑 출시 후 유심 카드 기반의 통신사와 앱카드 기반의 금융사로 전자지갑 시장이 양분됨
- SNS 업체 카카오는 국내 18개 은행과 금융결제원이 공동 개발한 NFC 기반의 모바일 전자지갑인 뱅크월렛카카오를 2014년 11월 출시하였음

○ 핀테크 보안기술

- 핀테크가 핫이슈로 떠오르는 가운데, 새로운 유형의 금융, 지불 방법에 대한 보안 제공이 관건이 되고 있음
- 애플 페이의 출시로 NFC 결제(3세대)가 이슈화되고 있어, 차세대 결제 기술인 BLE 기반 결제(4세대) 및 보안 기술 개발이 시도되고 있음
- 전통적 전자금융은 물론, 핀테크에서도 피싱/파밍, 메모리해킹은 보안 대책이 반드시 필요한 중요한 이슈임. 그러나, 주로 스타트업 등 보안 기술에 익숙하지 않는 핀테크 사업자의 특성상 필요한 보안 대책을 모두 구비하기에는 한계가 있어, 이를 해결하는 기술이 적용될 수 있음
- 다양한 유형의 핀테크 서비스 구조를 통해 유통되는 개인정보가 유출되고 악용될 가능성이 증가함. 따라서 개인정보 유통상 프라이버시 보호 기술의 적용성이 높음

3. 국내외 경쟁기관 현황

○ 인증/결제

- 삼성/LG 등의 휴대폰 제조사는 Google의 안드로이드 플랫폼을 적용한 스마트폰에서 NFC를 이용한 태그인식/정보 공유/결제 등 다양한 서비스를 제공함
- 삼성전자는 자사 휴대폰의 지문인식 기술 FIDO의 UAF 표준을 적용하여

Paypal과 함께 지불 솔루션을 개발하여 출시함

- SK플래닛/KT/LG 유플러스는 NFC와 독자 결제 프로세스를 활용한 전자지갑을 출시하였음
- 해외는 미국 유통업체들이 연합한 '머천트 커스터머 익스체인지(MCX)', 미국 통신업체들의 연합인 ISIS, Google, Microsoft, Visa 등이 독자적인 전자지갑 솔루션을 개발 중임
- 구글은 사용자인증 강화를 위한 5개년 로드맵을 설정했고, 그 기술로는 다중인증, OAuth인증, 위험기반 인증, 인증 연동기술, 공개키 기반 토큰 기술을 발전시킬 계획
- 미국 모바일 결제시장의 선두 주자 벤처기업 스퀘어(Square)가 GPS기술과 애플리케이션 기반 결제 방식을 접목해 큰 인기를 얻었고, 최근 스퀘어에서 iPad를 POS기기로 변환시킨 새 하드웨어 Square Stand를 출시 [KOTRA 해외비즈니스정보포털 '미국 전자지갑 열품, 모바일 결제시장 확대']

○ 안티 피싱/파밍

- QR코드를 이용한 스마트폰 인증/피싱 차단 솔루션은 Google의 SESAME, 홍코드의 댑코드, AuthmMe, Fonsign 등이 있으나 액티브피싱에는 무력함
- 미국의 Bank of America는 쿠키 기반의 개인화 이미지를 활용한 Sitekey를 피싱차단 서비스로 제공함
- RSA는 IP 주소를 이용하여 good/bad score를 할당하여 피싱사이트 여부를 서버에서 확인할 수 있는 Passmark 제품을 개발함
- 카카오는 카카오톡에서 가짜 친구를 쉽게 인식할 수 있는 스마트 인지 기술을 적용함
- 트위터는 서비스사이트에 올라오는 메시지 안에서 방문자를 유해SW나 개인정보 불법도용 사이트로 유도하는 링크를 걸러낼 수 있는 기술을 연구

적용함

- MS의 윈도우 10에서는 피싱 공격을 받았을 때 사용자의 ID를 보호하는 기능, 사용자 기기 자체와 PIN 혹은 바이오인증으로 구성된 2중인증 기능 등을 제공함

○ 빅데이터/SNS 프라이버시

- 마케토(Marketo)는 페이스북의 그래프서치가 이용자의 개인정보보호에 미치는 영향 및 개인정보보호 방법을 조언하기 위해 인포그래픽(Infographic)을 제작함. 그래프서치는 페이스북이 자체 개발한 소셜 검색 엔진으로 공유된 내용을 기반으로 사람, 사진, 장소 등을 검색 가능함
- 트룰리오의 프로필 플러스라는 서비스는 스팸용 가짜 Facebook 계정을 식별하여 광고비용에서 배재하는 기술인 필터링 서비스를 제공함
- 맥아피는 보안취약점 관련 데이터, 해결방법 등을 저장한 글로벌쓰렛인텔리전스(GTI)와 함께 방대한 로그데이터를 기존보다 2~3배 빠르게 처리하는 '나이트로'라는 빅데이터 솔루션을 접목하였음
- 시만텍은 자사가 보유하고 있는 인터넷 보안위협 데이터 수집 시스템 '글로벌 인텔리전스 네트워크'를 활용해 매일 80억 개가 넘는 보안위협을 분석하고 13억개 시스템을 통해 악성코드를 수집함
- 유럽의 Allow는 회원의 개인정보 판매를 대행하는 서비스로, 고객의 개인 관심사에 맞춘 광고를 보여주기 전에 허가를 요청하며, 마케팅 업체들로부터 고객의 개인정보를 제거하는 방식으로 개인정보의 가치를 높임
- ID 도용 등 제3자에 의한 개인 데이터의 무단 사용을 방지하기 위해 이용자를 대신하여 웹 상의 개인 데이터 사용을 모니터링해주는 서비스를 제공하는 업체로 씨에스아이덴터티(CSIdentity), 라이프락(LifeLock), 레퓨테이션닷컴(Reputation.com), 인텔리어스(Intelius) 등이 있음
- SNS, 콘텐츠 공유 사이트 등 공개된 개인 데이터를 수집하고 유료로 검색할 수 있게 하거나 광고주 등 제3자에게 판매하는 업체로는 인텔리어

스, 빈베리파이드(Been Verified), 스포키오(Spokeo), 애니후(Anywho), 스코피오(Scopeo), 화이트페이지즈(White Pages), 줌인포(ZoomInfo), 메디커넥트글로벌 (MediConnect Global) 등이 있음

제 3 절 기술개발 시 예상되는 기술적·경제적 파급 효과

1. 기술적 측면

○ 관계망(SNS)/스마트환경에 노출된 개인정보를 분석하여 위험을 평가하는 기술은 스마트지갑의 원천 보안기술로 활용 기대

○ 스마트환경에서의 프라이버시 보호 및 개인정보 유통을 위한 보안 핵심원천 기술과 지재권 확보

○ 시큐리티 큐레이션과 개인정보 유통 보안 기술 개발을 통해 관련 모바일 서비스 기술 분야에서 세계 수준의 기술경쟁력 확보 가능

[그림 1-4] 기술적 파급 효과

2. 경제적 산업적 측면

○ 개인정보 관리 분야의 시장규모는 2015년 세계 63.5조, 국내 1.2조원으로 예상되며, 세계시장 점유율 1% 확보 시 6천 3백억 원의 시장개척 가능

○ 프라이버시 우려로 침체되었던 관련 서비스 산업의 높은 성장과 고용을 촉진함

○ 핵심기술에 대한 중요 특허를 선점하고 기술 보급하여 국내 산업경쟁력 강화

○ 스마트 의료·헬스/금융/정부 등 사용자의 민감한 정보를 다루는 공공분야에서 뿐만 아니라, 정보수집 어려움으로 위치정보만을 사용하는 수준의 광고, 추천 등의 모바일 서비스를 고도화하기 위한 기반기술로 활용될 것임

[그림 1-5] 경제적 산업적 파급 효과

3. 사회적 측면

○ 온오프라인 피싱/사기, 개인정보 유출 등의 범죄 피해를 경감시킴

○ 온라인과 오프라인 환경에서 사용자 스스로 자기결정권을 가지고 정보를 공유, 제어할 공통 기술로 활용 예상

○ 인증정보의 유출 및 오남용에 취약한 지식기반 인증(예: 패스워드) 기술을 대체하여 생체기반 인증, 소지기반 인증 기술을 제공해 보안성과 편의성이 강화된 전자금융 서비스 활성화 기대

제 2 장 기술개발 내용 및 방법

제 2 장 기술 개발 내용 및 방법

제 1 절 최종 목표 및 평가 방법

1. 최종 목표

[표 2-1] 최종 목표

구분	내용
최종목표	○ 스마트 환경의 다양한 개체들로부터 안전하고 편리한 스마트 서비스를 제공받기 위해 리스크/협상에 기반한 시큐리티 큐레이션을 제공하는 프라이버시 강화형 개인정보 유통 보안 핵심 기술 개발 ○ End Product • 개인정보 (ID, 인증정보, 결제정보) 유통 보안 인터랙션 기술 (IPR, SW) • 온오프라인 피싱 방지 기술 (IPR, SW) • 개인정보 (노출, 연결, 추론) 공개 리스크 분석 기술 (IPR, SW) • 핵심기술 관련 국제특허 10건, 국내특허 17건, 표준 6건
세부목표	○ 주요 기능 • 개인정보 (ID, 인증정보, 결제정보) 유통 보안 인터랙션 기능 • 온오프라인 피싱 방지 기능 • 개인정보 공개 리스크 분석 기능 ○ 핵심 기술 • 개인정보 (ID, 인증정보, 결제정보) 유통 보안 인터랙션 기술 • 온오프라인 피싱 방지 기술

구분	내용
	• 개인정보 공개 리스크 분석 기술 ○ 적용서비스 • 스마트 의료·헬스/금융/정부 등 사용자의 민감한 정보를 다루는 공공분야에서 개인정보보호를 위한 기반 기술로 적용 • ATM, POS, 스마트패드, 사이니지 등 오프라인 환경의 스마트 단말을 통한 결제, 인증, 개인정보 공유를 위한 핵심 기술로 활용 • 사이트 로그인, 온라인 뱅킹, 모바일 본인인증 등 간편하고 보안이 강화된 사용자 인증을 요구하는 포탈, 금융, 통신 서비스 분야

2. 연구개발 추진 체계

가. 연구개발 추진 체계

[그림 2-1] 연구개발 추진 체계

나. 연구개발 방법

○ 한국전자통신연구원은 전체 연구 방향 설정 및 기술 개발 총괄

○ 한국전자통신연구원 주도로 개인정보 유통 보안 요소기술 개발 및 IPR 확보

- 온오프라인 피싱 방지 기술
- 개인정보 (노출, 연결, 추론) 리스크 분석 기술
- 개인정보 (ID, 인증정보, 결제정보) 유통 보안 기술

○ 관련 정부기관, 산업체, 유관기관, 학계와의 협력(공동연구, 위탁, 용역)을 통하여 요구사항을 도출하고, 상용화를 위해 필요한 요소를 적극 반영하여 기술 개발을 추진함

- 공동연구기관인 ㈜비씨카드와 요구사항 도출 및 스마트결제 응용서비스 시스템 개발
- 미래부/KISA/MOIBA와 공인인증서 정책, 기술개발 요구사항 협의 및 국제표준화 추진
- 안행부와 정부3.0 개인정보보호기술 및 요구사항 협의
- 금결원과 금융마이크로SD 및 공인인증서 관련 기술 개발 협력
- 외부 기관/업체의 요구사항을 수집하고 보유 서비스와 연계한 연구개발 수행
- 개발된 핵심 기술의 기술이전을 통해 상용화 및 응용서비스 구축 추진

○ 개인정보보호 분야는 관련 법/제도 전문가를 활용하여, 적법성 있는 기술 개발로 상용화 가능성을 높임

○ 유관기관 등을 활용해 산업계 현황과 상용화 시기 등을 파악하며, 개발기술을 홍보하여 기술보급과 확산을 견인함

○ 개인정보 유통 보안 요소 기술, 시스템 기술 등 상호운용이 요구되는 기술은 국내외 표준화 단체(W3C, TTA 등)를 통해 표준화 추진하며, 표준화 과정에서의 피드백을 기술 개발에 적극 반영함

○ 경쟁력 없는 요소기술은 공동연구기관, 전문업체 등에서 기 확보하고 있는 기술들을 활용, 본 과제는 핵심기술 개발에 집중하여 개발기간 단축함

3. 개발기술의 평가방법 및 평가항목

[표 2-2] 1차년도 성과 지표

성과목표		목표도출 근거	성과지표	당해 연도 목표 ('13년도)	평가(검증)방법	배점
output	시큐리티 큐레이션을 제공하는 프라이버시 강화형 개인정보 유통 보안 핵심 기술개발	국내 요소기술 기반이 부족하여 요소기술 개발과 지재권 확보의 의미를 가짐	개인정보 유통 인터랙션 시간(초)	3초 이내 (오프라인 자동화)	해당 목표기술에 대한 요구사항정의서 및 시험 결과서 제시	10
			개인정보 리스크 탐지율 (개인정보 탐지 종류)	7종 추출 (문장 분석)	해당 목표기술에 대한 요구사항정의서 및 시험 결과서 제시	10
			특허출원 건수(국내/국제)	7/4 건	특허 출원 증빙 자료 제시	20
			논문 건수	10 건	논문 증빙 자료 제시	10
			기술표준	2건	표준 증빙 자료 제시	10
			소계			60점
outcome/impact		요소기술 확보 및 일부 적용 단계이므로 기술 기반확보 여부와 공공 파급효과에 중점	기술이전 건수	1건	기술이전 증빙 자료 제시	20
			공공적/공익적 연구 성과 활용 실적	1건	공공 정책 반영 여부	20
			소계			40점
합계						100점

[표 2-3] 2차년도 성과 지표

성과목표		목표도출 근거	성과지표	당해 연도 목표 ('14년도)	평가(검증)방법	배점
output	시큐리티 큐레이션을 제공하는 프라이버시 강화형 개인정보 유통 보안 핵심 기술개발	국내 개인정보 유통 보안 기술 기반이 부족하여 핵심 기술의 구현과 지재권 확보 및 산업계에 기술 보급이 가능하도록 목표를 설정함	개인정보 유통 인터랙션 시간 범위 (초/m)	5m 이내 (정책 제어)	해당 목표기술에 대한 요구사항정의서 및 시험 결과서 제시	15
			개인정보 리스크 탐지율 (개인정보 탐지 종류)	개인정보 연결 3개도메인 (조합)	해당 목표기술에 대한 요구사항정의서 및 시험 결과서 제시	15
			특허출원 건수(국내/국제)	5/3 건	특허 출원 증빙 자료 제시	20
			논문 건수 (SCI/비SCI)	2/8 건	논문 증빙 자료 제시	10
			소계			60점
outcome/impact		핵심 기술 확보 및 일부 적용 단계이므로 상용화 가능성과 공공 파급 효과에 중점	기술표준 건수	2건	표준 증빙 자료 제시	15
			기술이전 수입액	0.7억원	기술이전 증빙 자료 제시	15
			공공적/공익적 연구성과 활용 실적 (정책반영/성과홍보/시범서비스)	1건	정책 반영 / 성과 홍보 / 시범서비스 여부	10
			소계			40점
합계						100점

[표 2-4] 3차년도 성과 지표

성과목표		목표도출 근거	성과지표	당해 연도 목표 ('13년도)	평가(검증)방법	배점
output	시큐리티 큐레이션을 제공하는 프라이버시 강화형 개인정보 유통 보안 핵심 기술개발	국내 개인정보 유통 보안 기술 기반이 부족하여 핵심 기술의 구현과 지재권 확보 및 산업계에 기술 보급이 가능하도록 목표를 설정함	개인정보 유통 보안 인터랙션 시간/범위 (초/m)	1.5m이내 (보안 협상)	해당 목표기술에 대한 요구사항정의서 및 시험결과서 제시	15
			개인정보 추론 리스크 탐지율/기능	이용자 단말 차단정보 종수 – 7종	해당 목표기술에 대한 요구사항정의서 및 시험결과서 제시	15
			특허출원 건수 (국내/국제)	5/3건	특허 출원 증빙 자료 제시	20
			논문 건수 (SCI/비SCI)	2/8건	논문 증빙 자료 제시	10
			소계			60점
outcome/impact		핵심 기술 확보 및 일부 적용 단계이므로 상용화 가능성과 공공 파급 효과에 중점	기술표준 건수	2건	표준 증빙 자료 제시	15
			기술이전 수입액	1억원	기술이전 증빙 자료 제시	15
			공공적/공익적 연구성과 활용 실적 (정책반영/성과홍보/시범서비스)	1건	정책반영/성과홍보/시범서비스 여부	10
			소계			40점
합계						100점

4. 정량적 성과 목표

[표 2-5] 성과 목표 및 달성치

구분	특허				논문		표준화	기술 이전	S/W 등록	기술문서
	국제		국내		SCI(E)	비SCI				
	출원	등록	출원	등록						
1차년도 (2013년)	4/0	/	7/8	/	/	10/11	2/9	1(0.5)/ 3(0.75)	3/24	50/53
2차년도 (2014년)	3/3	/	5/5	/	2/0	8/11	2/2	2(0.7)/ 5(3.15)	3/11	50/55
3차년도 (2015년)	3/2(1)	/	5/3(1)	/	2/4	8/8	2/3	2(1)/ 16(11.23)	3/4	50/30
합계	10/5(1)	/	17/16(1)	/	4/4	26/30	6/15	5(2.2)/ 24/(15.13)	9/39	150/138

* 특허 ( )는 현재 출원 중인 건수임

제 2 절 연차별 목표 및 평가 방법

1. 1차년도 목표 및 평가 방법

가. 개발 목표

○ 프라이버시 보호 모델 및 개인정보 유통 보안 요소기술 개발

- 개인정보 (ID, 인증정보, 결제정보) 유통 보안 요소기술 개발
- 스마트 환경의 프라이버시 보호 기반 기술 개발
- 개인정보 공개 리스크 분석 기술 개발

○ 개발 결과물

- 근접통신기반 개인정보 유통 인터랙션 모듈(SW, IPR)
- 온라인 피싱 방지 모듈(SW, IPR)
- 개인정보 공개 리스크 분석 모듈(SW, IPR)
- 특허(국내/국제) 7/4건, 표준 2건, 논문 10건

나. 평가 방법

○ 마일스톤 수행체계

마일스톤 번호	Milestone 명	수행기간		책임자
		시작일	종료일	
1	프라이버시 보호 모델 및 개인정보 유통 보안 요소기술 개발	2013.01.01	2013.12.31	진승헌
1.1	프라이버시 보호 모델 및 개인정보 유통 보안 요소기술 설계	2013.01.01	2013.07.31	진승헌
1.2	프라이버시 보호 모델 및 개인정보 유통 보안 요소기술 구현 및 시험	2013.08.01	2013.12.31	진승헌

○ 마일스톤 수행계획

Milestone No.	1.1
Milestone 명	프라이버시 보호 모델 및 개인정보 유통 보안 요소기술 설계
목표 일정	2013.07.31.
목 표	○ 개인정보 유통 보안 요소기술 개발 • 스마트 단말/서비스 식별 및 인증 기술 설계 • 근접통신기반 P2M/M2M 인터랙션 기술 설계 • 스마트지갑 개인정보 유통 보안 모델 분석 ○ 스마트 환경의 프라이버시 보호 기반 기술 개발 • 프라이버시 프레임워크 모델 분석 • 온라인 피싱 방지 기술 설계 ○ 개인정보 공개 리스크 분석 기술 개발 • 개인정보 특정 리스크 분석 기술 개발 • 개인정보 탐지 기술 개발
주요 결과물	1) 요구사항정의서 2) 기능정의서 3) 설계서

점검항목	점검기준	점검방법
요구사항 및 기능정의	○ 기술동향 분석 • 관련 기술동향 5개 이상 ○ 요구사항 분석 • 요구사항 수집 과정의 타당성: 검토회의 1회 이상 • 이용 시나리오 ○ 기능 정의 • 요구사항 반영여부	○ 기술동향 분석 • 기술동향 분석 TM 확인 ○ 요구사항 분석 • 요구사항정의서 확인 • 이용 시나리오 확인 • 요구사항정의서 회의록 ○ 기능 정의 • 요구사항정의서와 기능정의서 비교 확인
설계	○ 시스템 설계 • 설계서의 기능정의 반영여부 • 설계 타당성	○ 시스템 설계 • 기능정의서와 비교 확인 • 설계 회의록 및 조치 내역 확인

Milestone No.	1.2
Milestone 명	프라이버시 보호 모델 및 개인정보 유통 보안 요소기술 구현 및 시험
목표 일정	2013.12.31.
목 표	○ 개인정보 유통 보안 요소기술 개발 • 스마트 단말/서비스 식별 및 인증 기술 구현 • 근접통신기반 P2M/M2M 인터랙션 기술 구현 • 스마트지갑 개인정보 유통 보안 모델 도출 ○ 스마트 환경의 프라이버시 보호 기반 기술 개발 • 프라이버시 프레임워크 모델 도출 • 온라인 피싱 방지 기술 구현 ○ 개인정보 공개 리스크 분석 기술 개발 • 개인정보 특정 리스크 분석 구현 • 개인정보 탐지 모듈 구현
주요 결과물	1) 개인정보 유통 보안 및 리스크 탐지 분석 기술 (IPR, SW) 2) 시스템 시험절차서 3) 시스템 시험결과서

점검항목	점검기준	점검방법
개발 시스템 시험절차서 시험결과서	○ 핵심기술 개발 • 스마트 단말/서비스 식별 및 인증 모듈 구현 여부 • 스마트채널3 인증 모듈 구현 여부 • 개인정보 탐지 모듈 구현 여부 ○ IPR • 국내/국제 특허 7/4건 이상	○ 핵심기술 개발 • 기능 개발 검토 회의록 및 조치 내역 확인 • 시험결과서를 통해 해당 기능의 제공여부를 확인 ○ IPR • 특허 건수 확인

2. 2차년도 목표 및 평가 방법

가. 개발 목표

○ 연결/보안정책 기반 개인정보 유통 보안 시스템기술 개발

- 개인정보 (ID, 인증정보, 결제정보) 유통 보안 시스템 기술 개발
- 메모리해킹 피싱 공격 방지 기술 개발
- 개인정보 조합 리스크 분석 기술 개발

○ 개발 결과물

- 개인정보 (ID, 인증정보, 결제정보) 유통 보안 시스템 모듈 (SW, IPR)
- 메모리해킹 피싱 공격 방지 모듈(SW, IPR)
- 개인정보 조합 리스크 분석 모듈(SW, IPR)
- 특허(국내/국제) 5/3건, 표준 2건, 논문(SCI/비SCI) 2/8건

나. 평가 방법

○ 마일스톤 수행체계

마일스톤 번호	Milestone 명	수행기간		책임자
		시작일	종료일	
1	연결/보안정책 기반 개인정보 유통 보안 시스템 기술 개발	2014.01.01	2014.12.31	진승헌
1.1	연결/보안정책 기반 개인정보 유통 보안 시스템 기술 구현 및 시험	2014.08.01	2014.12.31	진승헌
1.2	연결/보안정책 기반 개인정보 유통 보안 시스템 기술 구현 및 시험	2014.08.01	2014.12.31	진승헌

○ 마일스톤 수행계획

Milestone No.	1.1
Milestone 명	연결/보안정책 기반 개인정보 유통 보안 시스템 기술 설계
목표 일정	2014.07.31.
목 표	○ 개인정보 (ID, 인증정보, 결제정보) 유통 보안 시스템 기술 개발 • In-Store 개인정보 유통 보안 인터랙션 기술 설계 • In-Store 스마트결제 시스템 기술 개발 설계 • 개인정보 유통 보안 시스템 기술 표준화 ○ 메모리해킹 피싱 공격 방지 기술 개발 • 메모리해킹 기반의 온라인 개인정보 탈취 모델 연구 • 악성코드 피싱/파밍 공격 방지 기술 설계 ○ 개인정보 조합 리스크 분석 기술 개발 • 개인정보 조합식별위험 분석 기술 설계 • 개인정보 정규화 탐지 모듈 설계 • 개인정보 필터링 기술 설계
주요 결과물	1) 요구사항정의서 2) 기능정의서 3) 설계서

점검항목	점검기준	점검방법
요구사항 및 기능정의	○ 기술동향 분석 • 관련 기술동향 5개 이상 ○ 요구사항 분석 • 요구사항 수집 과정의 타당성: 검토회의 1회 이상 • 이용 시나리오 ○ 기능 정의 • 요구사항 반영여부	○ 기술동향 분석 • 기술동향 분석 TM 확인 ○ 요구사항 분석 • 요구사항정의서 확인 • 이용 시나리오 확인 • 요구사항정의서 회의록 ○ 기능 정의 • 요구사항정의서와 기능정의서 비교 확인
설계	○ 시스템 설계 • 설계서의 기능정의 반영여부 • 설계 타당성	○ 시스템 설계 • 기능정의서와 비교 확인 • 설계 회의록 및 조치 내역 확인

Milestone No.	1.2
Milestone 명	연결/보안정책 기반 개인정보 유통 보안 시스템 기술 구현 및 시험
목표 일정	2014.12.31.
목 표	○ 개인정보 (ID, 인증정보, 결제정보) 유통 보안 시스템 기술 개발 • In-Store 개인정보 유통 보안 인터랙션 기술 구현 • In-Store 스마트결제 시스템 기술 개발 구현 • 개인정보 유통 보안 시스템 기술 표준화 ○ 메모리해킹 피싱 공격 방지 기술 개발 • 메모리해킹 기반의 온라인 개인정보 탈취 모델 도출 • 악성코드 피싱/파밍 공격 방지 기술 구현 ○ 개인정보 조합 리스크 분석 기술 개발 • 개인정보 조합식별위험 분석 기술 구현 • 개인정보 정규화 탐지 모듈 구현 • 개인정보 필터링 기술 구현
주요 결과물	1) 연결/보안정책 기반 개인정보 유통 보안 시스템 기술 (IPR, SW) 2) 시스템 시험절차서 3) 시스템 시험결과서 4) 표준기고서

점검항목	점검기준	점검방법
개발 시스템 시험절차서 시험결과서	○ 핵심기술 개발 • In-Store 개인정보 유통 보안 인터랙션 모듈 구현 여부 • 메모리해킹 피싱 공격 방지 모듈 구현 여부 • 개인정보 조합식별위험 분석 모듈 구현 여부 • 개인정보 필터링 탐지 모듈 구현 여부 ○ IPR • 국내/국제 특허 5/3건 이상 ○ 표준기고서 • 기술표준 2건 이상	○ 핵심기술 개발 • 기능 개발 검토 회의록 및 조치 내역 확인 • 시험결과서를 통해 해당 기능의 제공여부를 확인 ○ IPR • 특허 건수 확인 ○ 표준기고서 • 기술표준 건수 확인

3. 3차년도 목표 및 평가 방법

가. 개발 목표

○ 추론/보안협상 기반 개인정보 유통 보안 응용기술 개발

- 개인정보 (ID, 인증정보, 결제정보) 유통 보안 응용서비스 테스트베드 개발
- 개인정보 큐레이션 기술 개발
- 개인정보 추론 리스크 분석 기술 개발

○ 개발 결과물

- 개인정보 유통 보안 응용서비스 프로토타입 시스템 (SW, IPR)
- 개인정보 큐레이션 서비스(개인정보 지키미 앱) (SW, IPR)
- 개인정보 이상 접근행위 탐지 모듈 (SW, IPR)
- 국내/국제특허 5/3건, 표준 2건, 논문(SCI/비SCI) 2/8건

나. 평가 방법

○ 마일스톤 수행체계

마일스톤 번호	Milestone 명	수행기간		책임자
		시작일	종료일	
1	추론/보안협상 기반 개인정보 유통 보안 응용 시스템 기술 개발	2015.01.01	2015.12.31	진승헌
1.1	추론/보안협상 기반 개인정보 유통 보안 시스템 기술 설계	2015.01.01	2015.07.31	진승헌
1.2	추론/보안협상 기반 개인정보 유통 보안 시스템 기술 구현 및 시험	2015.08.01	2015.12.31	진승헌

○ 마일스톤 수행계획

Milestone No.	1.1
Milestone 명	추론/보안협상 기반 개인정보 유통 보안 응용 시스템 기술 설계
목표 일정	2015.07.31.
목 표	○ 개인정보 (ID, 인증정보, 결제정보) 유통 보안 응용서비스 테스트베드 개발 • 개인정보 유통 보안 응용서비스 프로토타입 설계 • In-Store 스마트결제 응용서비스 테스트베드 설계 • 개인정보 유통 보안 응용 기술 표준화 ○ 개인정보 큐레이션 기술 개발 • 오프라인 피싱 방지 기술 설계 • 개인정보 큐레이션 기술 설계 ○ 개인정보 추론 리스크 분석 기술 개발 • 개인정보 추론 탐지 리스크 분석 기술 설계 • 개인정보 이상 접근행위 탐지 프로토타입 설계
주요 결과물	1) 요구사항정의서 2) 기능정의서 3) 설계서

점검항목	점검기준	점검방법
요구사항 및 기능정의	○ 기술동향 분석 • 관련 기술동향 5개 이상 ○ 요구사항 분석 • 요구사항 수집 과정의 타당성: 검토회의 1회 이상 • 이용 시나리오 ○ 기능 정의 • 요구사항 반영여부	○ 기술동향 분석 • 기술동향 분석 TM 확인 ○ 요구사항 분석 • 요구사항정의서 확인 • 이용 시나리오 확인 • 요구사항정의서 회의록 ○ 기능 정의 • 요구사항정의서와 기능정의서 비교 확인
설계	○ 시스템 설계 • 설계서의 기능정의 반영여부 • 설계 타당성	○ 시스템 설계 • 기능정의서와 비교 확인 • 설계 회의록 및 조치 내역 확인

Milestone No.	1.2
Milestone 명	추론/보안협상 기반 개인정보 유통 보안 응용 시스템 기술 구현 및 시험
목표 일정	2015.12.31.
목 표	○ 개인정보 (ID, 인증정보, 결제정보) 유통 보안 응용서비스 테스트베드 개발 • 개인정보 유통 보안 응용서비스 프로토타입 구현 • In-Store 스마트결제 응용서비스 테스트베드 구현 • 개인정보 유통 보안 응용 기술 표준화 ○ 개인정보 큐레이션 기술 개발 • 오프라인 피싱 방지 기술 구현 • 개인정보 큐레이션 기술 구현 ○ 개인정보 추론 리스크 분석 기술 개발 • 개인정보 추론 탐지 리스크 분석 기술 구현 • 개인정보 이상 접근행위 탐지 프로토타입 개발
주요 결과물	1) 추론/보안협상 기반 개인정보 유통 보안 응용 시스템 기술 (IPR, SW) 2) 시스템 시험절차서 3) 시스템 시험결과서 4) 표준기고서

점검항목	점검기준	점검방법
개발 시스템 시험절차서 시험결과서	○ 핵심기술 개발 • 개인정보 유통 보안 응용서비스 프로토타입 구현 여부 • In-Store 스마트결제 응용서비스 테스트베드 구현 여부 • 오프라인 피싱 방지 기술 구현 여부 • 개인정보 큐레이션 서비스 구현 여부 • 개인정보 이상 접근행위 탐지 프로토타입 구현 여부 ○ IPR • 국내/국제 특허 5/3건 이상 ○ 표준기고서 • 기술표준 2건 이상	○ 핵심기술 개발 • 기능 개발 검토 회의록 및 조치 내역 확인 • 시험결과서를 통해 해당 기능의 제공여부를 확인 ○ IPR • 특허 건수 확인 ○ 표준기고서 • 기술표준 건수 확인

제 3 절 연차별 개발 내용 및 개발 범위

1. 1차년도 (2013)

가. 개발내용 및 범위

○ 개인정보 (ID, 인증정보, 결제정보) 유통 보안 요소기술 개발

- 스마트 단말/서비스 식별 및 인증 기술 개발
  - 터치사인(오프라인 전자서명) 기술 개발
- 근접통신기반 P2M/M2M 인터랙션 (결제/공유) 기술 개발
  - 표준POS 시스템 및 스마트영수증v2 기술 개발
- 스마트지갑 개인정보 유통 보안 모델 연구
  - 웨어러블 장치 기반 개인정보 유통 보안 모델(보안도우미) 연구

○ 스마트 환경의 프라이버시 보호 기반 기술 개발

- 스마트 환경용 프라이버시 정책 생성, 등록, 검증 프레임워크 (P4P) 모델 연구
- 온라인 피싱 공격 방지 기술 개발
  - 스마트채널2 고도화
  - 온라인 피싱 공격 기술 연구
  - 액티브 피싱 탐지, 상호인증 기능 제공

○ 개인정보 공개 리스크 분석 기술 개발

- 개인정보 특정 리스크 분석 기술 개발
  - 100만 샘플에 대한 개인 특정 리스크 (k-anonymity) 분석
- 개인정보 탐지 기술 개발
  - 개인정보 항목 별 노출 탐지

2. 2차년도 (2014)

가. 개발내용 및 범위

○ 개인정보 (ID, 인증정보, 결제정보) 유통 보안 시스템 기술 개발

- In-Store 개인정보 유통 보안 인터랙션 기술 개발
  - In-Store 통신 기반 개인정보 유통 보안 기술 (5m이내, MITM 공격 방지)
  - 정책기반 오프라인 프라이버시 보호 인터랙션 기술
- In-Store 스마트결제 시스템 기술 개발 (비씨카드)
  - In-Store 통신 기반 Check-in, Payment 시스템 기술 연구
  - 표준 POS 테스트베드 구축
- 개인정보 유통 보안 시스템 기술 표준화

○ 메모리해킹 피싱 공격 방지 기술 개발

- 메모리해킹 기반의 온라인 개인정보 탈취 모델 개발
  - 기존 안티 피싱/파밍 기술의 분석 및 취약점 도출
  - 취약점을 이용한 온라인 피싱 공격 툴킷 개발
- 악성코드 피싱/파밍 공격 방지 기술 개발
  - 악성코드에 대응하는 피싱/파밍 방지 인증 프로토콜 개발
  - 인증 프로토콜 안전성 분석

○ 개인정보 조합 리스크 분석 기술 개발

- 개인정보 조합식별위험 분석 기술 개발
  - 개인정보 조합식별위험 분석 기술 개발
- 개인정보 정규화 기술
  - 개인정보 탐지 정확률 개선
  - 탐지 비정형 개인정보 정규화 기술 개발
- 개인정보 필터링 기술 개발
  - 집적 데이터 개인정보 필터링 기술 개발

3. 3차년도(2015)

가. 개발내용 및 범위

○ 개인정보 (ID, 인증정보, 결제정보) 유통 보안 응용서비스 테스트베드 개발

- 개인정보 유통 보안 응용서비스 프로토타입 개발
  - BLE 통신 기반 개인정보 유통 보안 기술 (1.5m이내)
  - 유통 보안 인터랙션 응용서비스 프로토타입 개발
- In-Store 스마트결제 응용서비스 테스트베드 개발 (비씨카드)
  - 스마트결제 응용서비스 개발 (시스템 IF 및 POS단말 IF)
  - 스마트결제 시스템 필드 테스트 및 안정화
- 개인정보 유통 보안 응용 기술 표준화

○ 개인정보 큐레이션 기술 개발

- 오프라인 피싱 방지 기술 개발
  - 악성비콘 등의 피싱 공격에 대응하는 보안 프로토콜 개발
- 개인정보 큐레이션 기술 개발
  - 이용자 단말 민감정보 노출 차단 기술 개발
  - 이용자 단말 지키미 앱 개발

○ 개인정보 추론 리스크 분석 기술 개발

- 개인정보 추론 탐지 리스크 분석 기술 개발
  - 관계, 속성 기반 개인정보 추론 기술 개발
  - 개인정보 탐지 기술 고도화
- 개인정보 이상 접근행위 탐지 프로토타입 개발
  - 이상 접근 행위 탐지 기술
  - 개인정보 접근 모니터링 인터페이스 개발

제 3 장 연구 개발 결과

제 3 장 연구 개발 결과

제 1 절 1차년도 연구개발 결과

1. 1차년도 연구개발 추진 일정

[표 3-1] 1차년도 연구개발 추진 일정

과제내용	추진일정 2013년 1	2	3	4	5	6	7	8	9	10	11	12	활동 책임자	연구 개발비 (천원)	참여 인력 (M/Y)
개인정보 유통보안 요소 기술 개발 - 스마트 단말/서비스 식별 및 인증 기술 개발 - 근접통신기반 P2M/M2M 인터랙션 기술 개발 - 스마트지갑 개인정보 유통 보안 모델 연구 - 유통단말 인터페이스 표준화 - 개인정보(결제정보) 관리 표준화	→	→	→	→	→	→	→	→	→	→	→	→	진승헌 (김수형) (장석호)	768,889 (200,000)	3.89 (1.5)
스마트 환경의 프라이버시 보호 기반 기술 개발 - 프라이버시 프레임워크 모델 연구 - 온라인 피싱 방지 기술 개발					→	→	→	→	→	→	→	→	진승헌 (김승현)	480,556	2.43
개인정보 공개 리스크 분석 기술 개발 - 개인정보 특정 리스크 분석 기술 개발 - 개인정보 탐지 기술 개발	→	→	→	→	→	→	→	→	→	→	→	→	진승헌 (최대선)	480,556	2.43
주요 Milestone 완성점에서의 수행결과	- 요구사항 정의서 - 기능 정의서 - 설계서 - 특허 : 4건 - 논문 : 4건 - 표준기고서 : 2건 - 기술문서 : 38건								- 시험절차서 - 시험결과서 - 특허: 4건 - 논문: 7건 - 표준기고서:7건 - 기술문서: 15건 - SW 등록: 24건 - 기술이전:3건						
합계														1,930,000	10.26

2. 1차년도 연구개발 추진 실적

[표 3-2] 연구개발 추진 실적

목 표	세 부 계 획	실 적
프라이버시 보호 모델 및 개인정보 유통 보안 요소기술 개발 (정량적 성과)	○ 특허 - 국내 특허 출원 7건 - 국제 특허 제출 4건 ○ 논문 - 비SCI 10건 ○ 표준화 - 기고서 2건 ○ 기술이전 1건 ○ S/W등록 3건 ○ 기술문서 50건	○ 특허 - 국내 특허 출원 8건 ○ 논문 - 비SCI 국제 1건 - 비SCI 국내 10건 ○ 표준화 - 국내 표준안 7건 채택 - 국제 기고서 2건 채택 ○ 기술이전 3건 ○ S/W등록 24건 ○ 기술문서 53건
요구사항 분석 및 기능 정의	○ 1차년도 요구사항 정의 ○ 2차년도 기능 정의	○ 요구사항 정의서 (기술문서) - 사용자 요구사항 - 시스템 요구사항 ○ 기능 정의서 (기술문서) - 개인정보유통보안 - 온라인 피싱 방지 - 개인정보 리스크 탐지 ○ 논문 - 모바일 전자 영수증 - 액티브 피싱 공격 및 대응방안 고찰 - 빅데이터 개인정보 위험 분석 기술 - 금융기관을 타켓으로 하는 피싱/파밍 공격 기술 동향 - 소셜네트워크서비스 개인정보 노출 실태 분석

목 표	세 부 계 획	실 적
		- 비정형 사용자 이름의 정형화된 한글 이름 변환 방법 연구 - 페이스북과 트위터 이용자 계정 연결 방법 - 자동 구축된 코퍼스를 이용한 비정형 개인정보 탐지 기법 (우수논문수상) - 공공정보 개방 공유에 따른 개인정보보호 기술 검토 (우수논문수상) - SNS에 노출된 개인정보의 소유자 식별 방법 - Geo-Location based QR-Code Authentication Scheme to Defeat Active Real-Time Phishing Attack (ACM CCS-DIM) ○ 기술문서 - 액티브 피싱 공격 및 대응방안 고찰 - 잊혀질 권리의 개념 및 방향 고찰 - 개인정보 공유 고찰 - 모바일 ID 및 스마트 영수증 소개 - OAuth 2.0 소개 - 웹 서비스 한글 처리 - GCM 사용법 - ID 서버 프로토타입 설계 - 금융 마이크로 SD 개발환경 구축 - 웹 서비스 서블릿 간 사용자 정보 공유 방법 - PostgreSQL 문법 정리 - Python Tutorial 정리 - Python 정규식(Regular Expresstion) 모듈 정리 - 통계 학습을 위한 Scikit-learn - 트위터 샘플에 대한 이메일 추출 방법

목 표	세 부 계 획	실 적
		및 분석 결과 - SNS 보안 이슈 및 기술 동향 - 사용자 IP 주소를 이용한 피싱 방지 기법 - 피싱 방지를 위한 OTP 이용 서버 인증 기법 제안 - Contextual OTP - A secure cookie scheme - OCR 테스트 - 온라인 터치사인 등록 - 스마트 지갑과 위치 기반 서비스 - 위치 정보 프라이버시 기술 - POS 보안기술 현황 - 오프라인 보안 이슈 - 클라우드ID카드 기술 개요 - 터치사인 시나리오 - NFC, 결제 그리고 그 다음 - 웨어러블장치 기반의 인증서비스 - 터치사인 서버 시나리오 - 스마트영수증2 UX - 씬클라이언트 환경에서 공인인증서 사용방안 검토 - 씽크풀 위치기반 인증 솔루션 분석 - FIDO 얼라이언스 프로젝트 분석 - 월간 ETRI 인증실 뉴스레터-2013년 3월 - 월간 ETRI 인증실 뉴스레터-2013년 4월 - 월간 ETRI 인증실 뉴스레터-2013년 5월 - 월간 ETRI 인증실 뉴스레터-2013년 6월 - 월간 ETRI 인증실 뉴스레터-2013년 7월

목 표	세 부 계 획	실 적
		- 월간 ETRI 인증실 뉴스레터-2013년 8월 - PKI 기술 및 NPKI 이슈 - W3C Webcrypto WG 소개 - WebCert관련 Same Origin Policy 이슈분석 - PKCS#11 소개 - 액티브피싱-하나은행 - 액티브피싱-우리은행
시스템 설계	○ 개인정보유통보안 설계 ○ 온라인 피싱 방지 설계 ○ 개인정보 리스크 탐지 설계	○ 시스템 설계서 (기술문서) ○ 개인정보유통보안 - 터치사인 인증서 관리 . 터치사인 앱 설치 . 인증서 등록 . 인증서 관리 - 터치사인 인증서 사용 . 전자서명(인증서카드) . 전자서명(인증서SD) . 전자서명(서비스단말) . 전자서명(전화번호) . 로그인 - 유통 보안 . 클라우드ID를 이용한 사용자 및 서비스 단말 식별과 인증 - 웨어러블 장치 기반의 인증서비스 설계 . 모바일 단말 전자서명 데이터 변경 방지 기능 설계 . 사용자 인증정보 웨어러블 관리 및 통신 기능 설계

목 표	세 부 계 획	실 적
		○ 온라인 피싱 방지 - 스마트채널 프로그램 . 보안로그인 - 처음 사용 PC . 보안로그인 - 재사용 PC - URL 인식 . URL 인식 . URL 검증 ○ 개인정보 리스크 탐지 - 문장분석 개인정보 추출 . 개인정보 추출 . 소유자 분류 . 위험도 산정 - 리스크 시각화 . 개인정보 노출 현황 시각화 . 개인정보 필터링
시스템 구현	○ 개인정보유통보안 구현 ○ 온라인 피싱 방지 구현 ○ 개인정보 리스크 탐지 구현	○ 프로그램 - 개인정보유통보안 . 터치사인 서버 . 터치사인 클라이언트 . 터치사인 응용 어플리케이션 . 터치사인 프로토콜 라이브러리 . 클라우드아이디 서버 . 클라우드아이디 포스 . 클라우드아이디 클라이언트 . 클라우드아이디 벤딩머신 . 클라우드아이디 라이브러리 . 모바일 전자영수증 앱 . 모바일 전자영수증 표준 라이브러리 . 휴대폰 인증 보안 도우미 . 거래내역확인 보안 도우미 - 온라인 피싱 방지 . 스마트채널 서버 . 스마트채널 클라이언트

목 표	세 부 계 획	실 적
		. 스마트채널 웹 주소 인식 - 개인정보 리스크 탐지 . 데이터 추출 . 개인정보 추출 . 정보 소유자 식별 . 이메일 정보 추출 . 영문이름 한글 변환 . 티에프-아이디에프 산출 . 개인정보 관계형 데이터베이스 관리 . 개인정보 위험도 탐지 필터 서버
표준화 추진	○ 국내 표준 - 표준안 채택 1건 ○ 국제 표준 - 기고서 채택 1건	○ 국내 표준안 7건 채택 - NFC P2P기반 모바일 전자 영수증 관리 규격 (TTAK.KO-12.0224) - POS 단말기 사용자 인터페이스 (TTAK.KO-12.0217) - POS 단말기 결제모듈 인터페이스 (TTAK.KO-12.0227) **- 모바일 단말을 이용한 디바이스 제어 프로토콜 및 보안 기능 (TTAK.KO-12.0225) (표준특허)** - 자바 스크립트 객체 표기법(JSON) 웹 전자서명 (TTAE.OT-12.0018) - 자바 스크립트 객체 표기법(JSON) 웹 키 (TTAE.OT-12.0017) - 자바 스크립트 객체 표기법(JSON) 객체 서명 및 암호화 사용 시나리오 및 요구사항 (TTAE.OT-12.0016) ○ 국제 기고서 2건 채택 - W3C. Web Certificate API 표준 초안 - W3C. Web Certificate API 표준 수정안

목 표	세 부 계 획	실 적
		○ 의장단 진출 : 3건 - W3C Editor : 조상래 - TTA PG502 의장 : 진승헌 - TTA PG502 간사 : 조상래

3. 각 기관/기업별 추진 내역

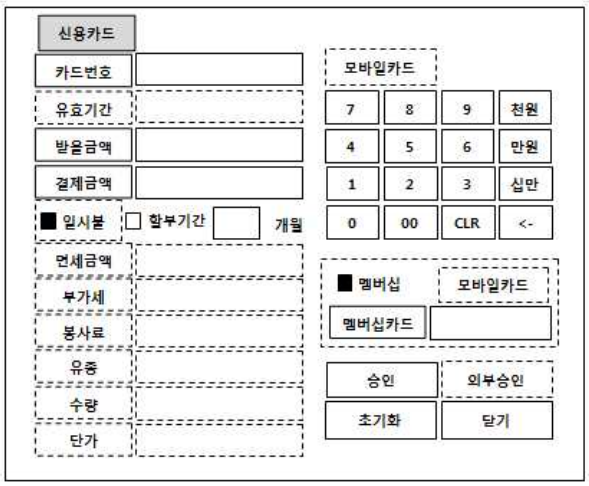
가. 스마트결제/공유를 위한 단말 인터페이스 개발

공동연구기관: (주)비씨카드

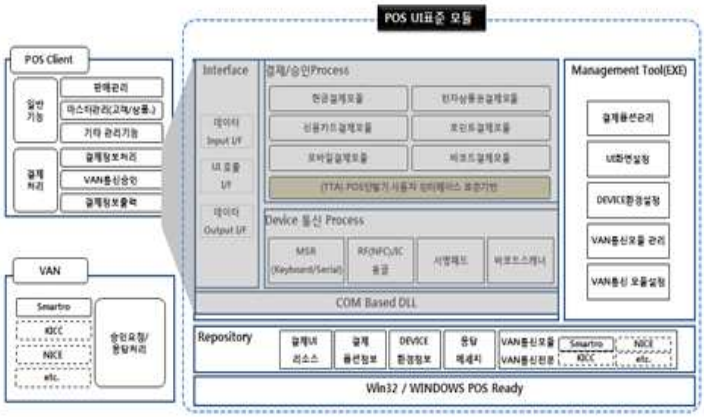
○ 연구개발 배경 및 연구목표

- 연구개발 배경 및 필요성
  - 모바일카드나 바코드 결제 등 신규 결제수단으로 결제 시 소비자 혼란 초래
  - POS 시스템에 의한 고객의 신용카드 정보 유출 우려
- 연구목표
  - POS 결제 표준 UI/UX 개발
  - 업계를 리딩해 갈 수 있는 결제플랫폼 개발
  - 향후 이슈가 될 것으로 예상되는 IC카드 승인거래를 포함하여 개발

○ 연구 내용 및 협력 현황



[그림 3-1] POS 표준 사용자인터페이스 화면



[그림 3-2] POS 표준 Architecture

- POS 결제 표준 UI / UX 기술 연구
- 업계를 리딩해 갈 결제플랫폼 개발
- POS 결제플랫폼 인터페이스 개발

○ 연구개발 효과

- 지급결제 용어통일, POS사용화면 표준화로 사용자 편의개선 및 고객 불편사항 청취, 이해하는 데 도움
- 밴사 <-> 단말기 <-> 서명패드, 동글 간 인터페이스 표준지원으로 POS 개발편의성, 유지관리 시간, 비용 절감
- POS기반 신규 가맹점서비스 개발 효율성 제고

○ 협력연구 결과물

- 금융 지급결제 산업내 POS관련 TTA 정보통신기술단체 표준 등록
- POS UI/UX, Interface 표준에 대한 결제플랫폼 라이브러리 개발
- POS 결제플랫폼 내 차세대모바일카드, 스마트영수증 규격 반영

4. 기술개발 결과의 유형 및 무형 성과

가. 특허

: 국내 출원8건

1) 웹 사이트 검증 장치 및 그 방법

2) 클라우드 ID 카드를 이용하여 개인 정보를 제공하기 위한 시스템 및 그 방법

3) 모바일 기기의 유해 정보를 검증하기 위한 시스템 및 그 방법

4) 사용자 단말을 통해 IC 카드를 관리하고 이용하는 방법 및 장치 (S등급)

5) 개인정보 소유자 식별 장치 및 방법

6) 보안 도우미 서비스 제공장치 및 서비스 제공방법

7) 코퍼스 자동 구축 방법 및 이를 이용한 개체명 인식 방법과 장치

8) 휴대 단말기, 단말기 및 보안쿠키를 이용한 인증 방법

나. 프로그램

: 등록 24건

○ 개인정보 유통 보안

1) 터치사인 서버

- Push 서비스를 이용한 터치사인 응용을 위한 서버
- 사용자 로그인 처리 및 클라이언트 Push 서비스

2) 터치사인 클라이언트

- 터치사인을 이용한 로그인 및 전자서명
- 인증서 관리

3) 터치사인 응용 어플리케이션

- 서비스는 사용자 입회 시스템
- 전자서명/요청/응답 기능

4) 터치사인 프로토콜 라이브러리

- 프로토콜 메시징 생성 및 처리
- 터치사인 메시지 생성 및 처리

5) 클라우드아이디 서버

- 클라우드 ID 시스템에서 사용자 정보를 관리하는 서버
- Push 서비스를 이용한 클라우드 ID 서버

6) 클라우드아이디 포스

- 개인정보를 요청하는 POS 시스템
- 클라우드 ID 프로토콜 처리
- 클라우드 ID 서버로 성인인증 요청

7) 클라우드아이디 클라이언트

- 개인정보 공유 동의
- 개인정보 동의 로그 관리
- GCM 메시지 수신/스마트폰 웨이크업

8) 클라우드아이디 벤딩머신

- 클라우드 ID 프로토콜 처리
- 클라우드 ID 서버로부터 수신한 결과에 따라 서비스 제공

9) 클라우드아이디 라이브러리

- 클라우드 ID 정의 및 데이터 생성
- 프로토콜 메시지 생성

10) 모바일 전자영수증 앱

- POS로부터 전자영수증을 수신함
- 모바일 전자영수증 관리 및 수신

11) 모바일 전자영수증 표준 라이브러리

- TTA 표준에 맞도록 구현
- 모바일 전자영수증 포맷 및 메시지 생성/처리

12) 휴대폰 인증 보안 도우미

- 휴대폰 인증 프로토콜
- 보안도우미 연동 서비스

13) 거래내역확인 보안 도우미
- 거래 내역 전송 프로토콜
- 보안도우미를 이용한 거래내역 확인

○ 온라인 피싱 방지

14) 스마트채널 서버
- 액티브피싱 방지를 위한 보안 쿠키 사용
- 사용자 인증 및 스마트 채널 인증

15) 스마트채널 클라이언트
- 바코드 스캔
- 사용자 인증 및 접속한 PC 관리

16) 스마트채널 웹 주소 인식
- 카메라를 이용한 이미지 획득
- OCR 인식 및 이미지 전/후처리

○ 개인정보 리스크 탐지

17) 데이터 추출
- NER 결과에서 직장/직업 추출
- 트위터 파일에서 전화번호 추출
- SNS 데이터에서 이름 추출

18) 개인정보 추출
- 비정형개인정보 추출
- 추출 정확도 측정 및 출력

19) 정보 소유자 식별
- 추출된 정보에 대한 주체를 식별

- 주체는 문장을 작성한 본인 또는 제 3자로 구분

20) 이메일 정보 추출

- 비정형 문장에 노출된 다양한 형태의 이메일 정보 추출

21) 영문이름 한글 변환

- 영문이름을 정형화된 한글 이름 변환

22) 티에프-아이디에프 산출

- N-gram 형태의 Feature 추출
- 문장에서 추출할 수 있는 모든 Feature에 대한 TF-ITF 값 산출

23) 개인정보 관계형 데이터베이스 관리

- SNS에 노출된 개인정보 관리 및 시각화
- 수집된 데이터 관리를 위한 RDB 테이블 구성

24) 개인정보 위험도 탐지 필터 서버

- 범죄 분야별 위험도 산출
- 주민번호 유추 가능성 산출
- 개인정보 노출에 따른 경고 및 필터 기능

다. 논문

: 국제 1편, 국내 10편

1) 모바일 전자 영수증, TTA 저널
2) 액티브 피싱 공격 및 대응방안 고찰, 정보통신동향분석
3) 빅데이터 개인정보 위험 분석 기술, 정보보호학회지
4) 금융기관을 타켓으로 하는 피싱/파밍 공격 기술 동향, 대한전자공학회지
5) 소셜네트워크서비스 개인정보 노출 실태 분석, 정보보호학회 논문지
6) 비정형 사용자 이름의 정형화된 한글 이름 변환 방법 연구, 정보과학회 추계 학술대회
7) 페이스북과 트위터 이용자 계정 연결 방법, 정보과학회추계학술대회

8) 자동 구축된 코퍼스를 이용한 비정형 개인정보 탐지 기법, 정보과학회추계학술대회 (우수논문수상)

9) 공공 정보 개방 공유에 따른 개인정보보호 기술 검토, 정보과학회추계학술대회 (우수논문수상)

10) SNS에 노출된 개인정보의 소유자 식별 방법, 정보보호학회 논문지

11) Geo-Location based QR-Code Authentication Scheme to Defeat Active Real-Time Phishing Attack, ACM CCS DIM

라. 국내 표준화

: TTA 표준안 채택 7건

1) NFC P2P기반 모바일 전자 영수증 관리 규격

- 모바일 전자 영수증 관리를 위한 모바일 앱이 공통적으로 제공 하는 기능 정의
- 모바일 전자 영수증의 활용 범위를 확대하고 관련 부가 서비스 개발에 기여

2) POS단말기 사용자 인터페이스

- 스마트 POS단말기를 위한 통일된 화면UI 및 결제방법 UX 정의
- 스마트결제 등 새로운 기술적용에 따른 가맹점/고객의 이용혼란 방지

3) POS단말기 결제모듈 인터페이스

- 스마트 POS단말기의 결제관련 모듈에 대한 인터페이스 정의
- 스마트지갑 기술 확산, 관련업계 요구사항 반영에 기여

4) 모바일 단말을 이용한 디바이스 제어 프로토콜 및 보안 기능 (표준특허)

- 스마트폰과 디바이스간 제어 프로토콜 정의
- 단일 어플리케이션으로 복수 개의 디바이스를 제어

5) 자바 스크립트 객체 표기법(JSON) 웹 전자서명

- JSON으로 표기된 내용을 전자서명하기 위한 구조체를 정의
- RFC 표준으로 영문표준의 국내수용임

6) 자바 스크립트 객체 표기법(JSON) 웹 키

- 전자서명에 필요한 공개키와 인증서에 대한 JSON 구조체를 정의
- RFC 표준으로 영문표준의 국내수용임

7) 자바 스크립트 객체 표기법(JSON) 객체 서명 및 암호화 사용 시나리오 및 요구사항

- JSON 기반의 전자서명과 암호화를 사용하는 시나리오 설명과 요구사항을 정의
- RFC 표준으로 영문표준의 국내수용임

마. 국제 표준화

: W3C 국제 기고서 채택 2건

1) Web Certificate API 표준 초안

- 액티브 X 이용없이 웹브라우저에서 인증서 관리(발급/갱신/폐기) 기능을 제공하는 기술
- 웹 기반의 인증서 관리 기능을 제공하는 자바 스크립트 API 정의

2) Web Certificate API 표준 수정안

- 인증서 관리 API 업데이트 및 서버와 교환하는 메시지 형식을 정의하는 기고서

[그림 3-3] W3C TPAC Web Crypto WG 회의

바. 기술이전

: 기술이전 3건 완료

1) 기술이전명: 스마트채널3 및 개인정보 추출 모듈 세부 기술 중

A. 스마트채널 3 기술

- 3,000만원

2) 기술이전명: 스마트채널3 및 개인정보 추출 모듈 세부 기술 중

B. 개인정보 추출 모듈

- 3,000만원

3) 기술이전명: 웨어러블 장치를 이용한 거래내역확인 및 휴대폰 인증 기술

- 1,500만원

사. 상용화 지원

1) SC제일은행의 QR코드 로그인

- 2013.4.15. SC제일은행 스마트채널 기술이 적용됨

[그림 3-4] SC제일은행 QR코드 로그인

2) 소프트포럼의 '제큐어투웨이' 출시

- 2013.9.10. 소프트포럼의 2채널 인증 솔루션으로 적용됨

소프트포럼, 인터넷 금융사기 대응 솔루션 '제큐어투웨이' 출시

PC와 스마트폰 등 2개 이상 인증 통해 안전한 금융거래 지원

2013년 3월 10일 (화) 14:55:13

[아이티데일리] 소프트포럼(대표 이경룡)은 최근 피해 사례가 급증하고 있는 메모리 해킹은 물론 실시간 피싱에 이르기까지 다양한 인터넷 금융사기 수법에 대응할 수 있는 신제품 'Xecure2way(제큐어투웨이)'를 출시한다고 10일 밝혔다.

제큐어투웨이는 사용자들이 안전하게 금융거래를 할 수 있도록 해주는 투채널 인증 솔루션으로, PC와 스마트폰 등 2개의 채널에서 거래 내역 인증을 받아야만 금융 거래가 진행되도록 만든 솔루션이다.

예를 들어, 사용자가 계좌 이체를 실행할 때 PC상의 암호화된 QR 코드를 통해 스마트폰에서 금융 거래 내역을 확인한다면, 이 때 확인된 내역과 서버에 수신된 금융 거래 내역이 일치해야만 금융 거래가 정상적으로 이루어진다.

해커가 변조한 금융 거래 내역이 서버와 스마트폰 상에서 일치할 수 없기 때문에, 현재 문제가 되고 있는 메모리 해킹 및 해외에서 발견된 실시간 피싱에 이르기까지 큰 피해를 야기하는 금융거래 사기를 차단할 수 있다.

소프트포럼의 암호화 기술을 통해 QR코드 변조를 방지하고, 사용자 및 서버의 이중 인증을 통해서 거래 내역이 확인되기 때문에 기존의 SMS 인증이나 OTP 등 PC 단에서만 이루어지는 인증보다 한층 강화된 보안성을 제공한다.

[그림 3-5] 소프트포럼의 '제큐어투웨이'

아. 전시회 참가

1) 세계 보안 EXPO 2013

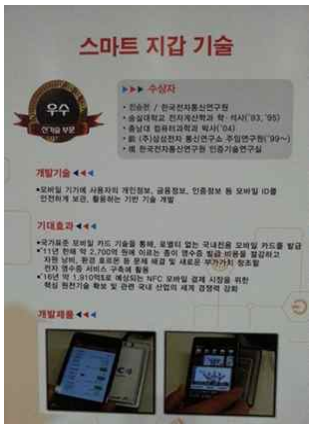
- 2013.3.5.~3.8, KINTEX

[그림 3-6] 세계 보안 EXPO 2013

2) 대한민국 R&D 성과 전시회

- 2013.11.12.~11.14. KINTEX

- 산업기술상 수상



[그림 3-7] 대한민국 R&D 성과 전시회

자. 보도 자료

○ SNS에서 공개되는 개인 정보를 추출하고 위험을 분석

- KBS, MBC 외 27개 신문에 “SNS 통한 개인정보 노출 심각‘ 기사

[그림 3-8] 보도 자료

차. 수상 내역

○ 미래부 장관상. 2013.7.10.

○ 특허청장상. 2013.5.15.

○ ICT R&D 우수성과상. 2013.11.12.

○ 이달의 산업기술상. 2013.10.29.

○ 경제과학대상. 2013.12.3.

[그림 3-9] 수상 내역

카. 기술 동향 분석

○ 뉴스레터 발간

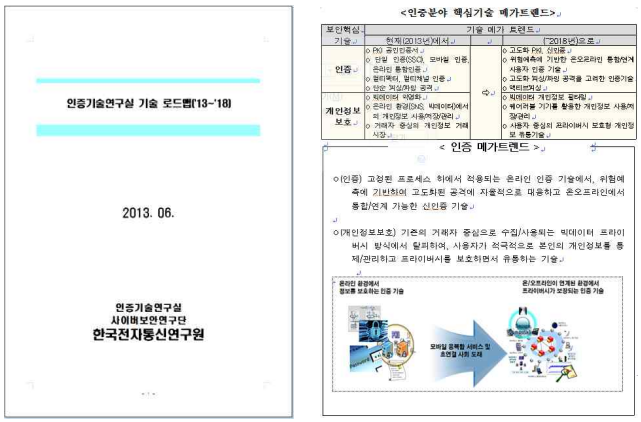
- 인증, 피싱, 프라이버시 과제와 연관된 기술 동향에 대해 지속적인 모니터링
- 주간 뉴스레터: 48회　　월간 뉴스레터: 7회

[그림 3-10] 뉴스레터 발간

○ 기술 로드맵

- 인증분야의 핵심 기술로 '인증', '개인정보'를 선정하고 메가트렌드를 정의함
- 인증, 안티 피싱/파밍, 개인정보 유통보안, 아이덴터티 분석 분야의 시장/기술동향 분석

- 각 분야별로 세부기술을 검토하여 중점추진과제 9개 도출



[그림 3-11] 기술 로드맵

타. 시스템 개발

1) 터치사인 시스템

○ 개발 내용

- 오프라인 환경에서도 사용자가 소지한 휴대폰 또는 현금카드(스마트카드)로 안전하게 전자서명 가능한 NFC 기반 인증서 관리 및 이용 기술 구현
- 공인인증서를 금융마이크로SD 또는 현금카드(스마트카드)에 발급 관리할 수 있는 모바일 CMP(Certificate Management Protocol) 기능을 사용자 휴대폰에 탑재
- 현금카드(스마트카드)가 분실, 악용되는 것을 방지하기 위해 등록 휴대폰에서만 전자서명 가능한 보안 기능을 제공
- 현금카드(스마트카드)를 간편 로그인 또는 거래 인증(본인 확인)에 사용할 수 있는 보안 기능을 제공

[그림 3-12] 터치사인 개념도

[그림 3-13] 터치사인 시연 화면

○ 개인정보 유통보안 인터랙션 시간

- 입회신청 서류 문서를 위한 오프라인 전자서명 기술

○ 시험 환경

- 공인인증서 규격 준수
- 공인인증서 키사이즈 2,048bytes

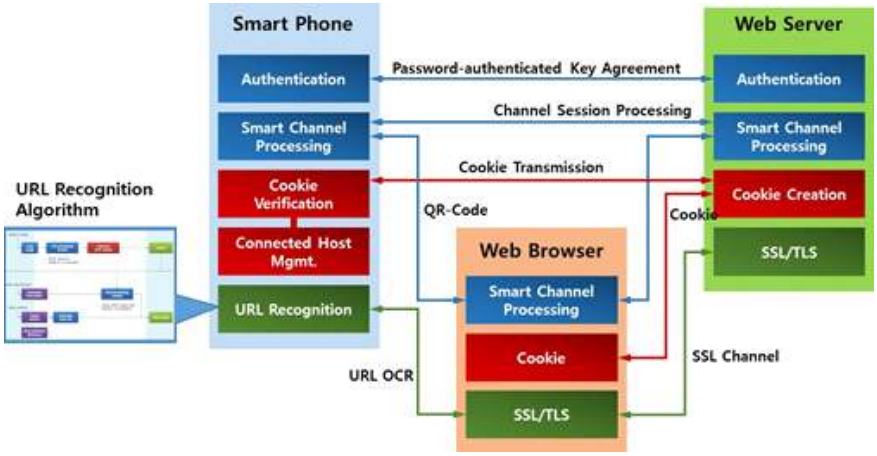
- 전자서명 알고리즘 SHA256, RSA
- 보안토큰(카드 내에서 전자서명). 금융IC카드 규격

[그림 3-14] 오프라인 인터랙션 시간

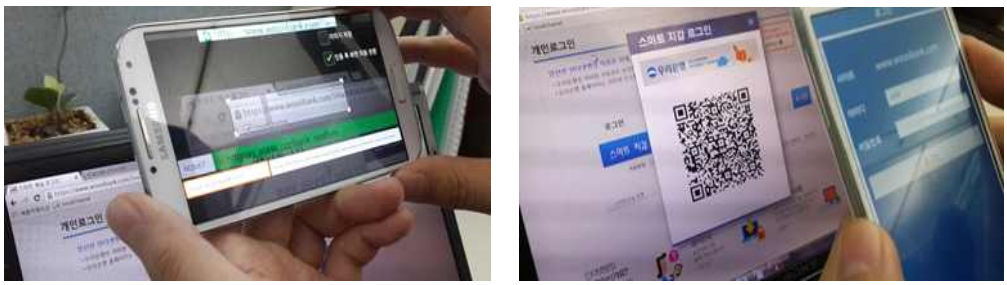
2) 스마트채널3 구현

○ 개발 내용

- QR코드를 이용하여 웹브라우저의 인증 절차를 스마트폰에서 대신 처리하는 서비스로, 상호인증 프로토콜과 보안토큰을 통해 서버/클라이언트가 안전하고 편리하게 인증하는 기능 구현
- 보안쿠키를 통해 사용자 PC를 등록하고, 기존의 persistent cookie의 문제였던 재사용 공격과 보안키 관리 이슈를 해결함
- 스마트폰 카메라를 이용하여 웹브라우저의 URL 주소를 자동으로 인식하고, 서버의 URL 주소와 일치여부 판별 및 피싱사이트의 주소 패턴을 고려한 피싱 차단 기능 구현



[그림 3-15] 스마트채널3 구조

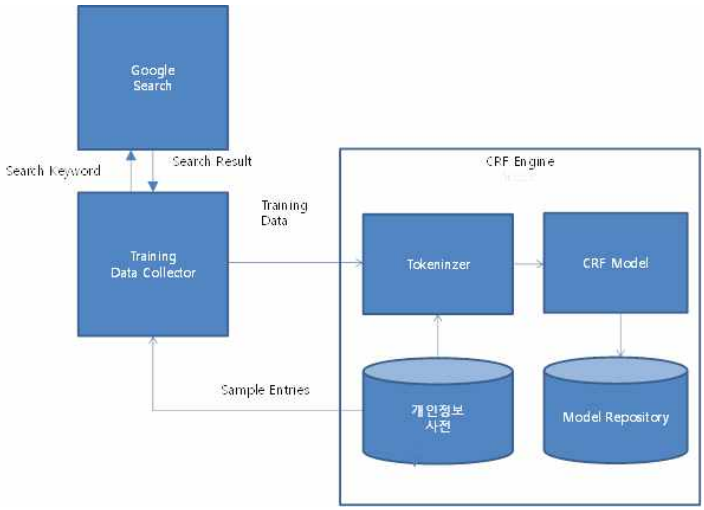


[그림 3-16] 스마트채널3 시연 화면

3) 개인정보 공개 리스크 분석 기술 개발

○ 비정형 개인정보 탐지

- 이름, 지역, 직업, 학교, 직장 등의 비정형 개인정보 탐지



[그림 3-17] 개인정보 탐지 모듈

○ 개인정보 위험도 분석

- 개인 특정 위험 분석

[그림 3-18] 개인정보 특정 위험 분석 결과-페이스북

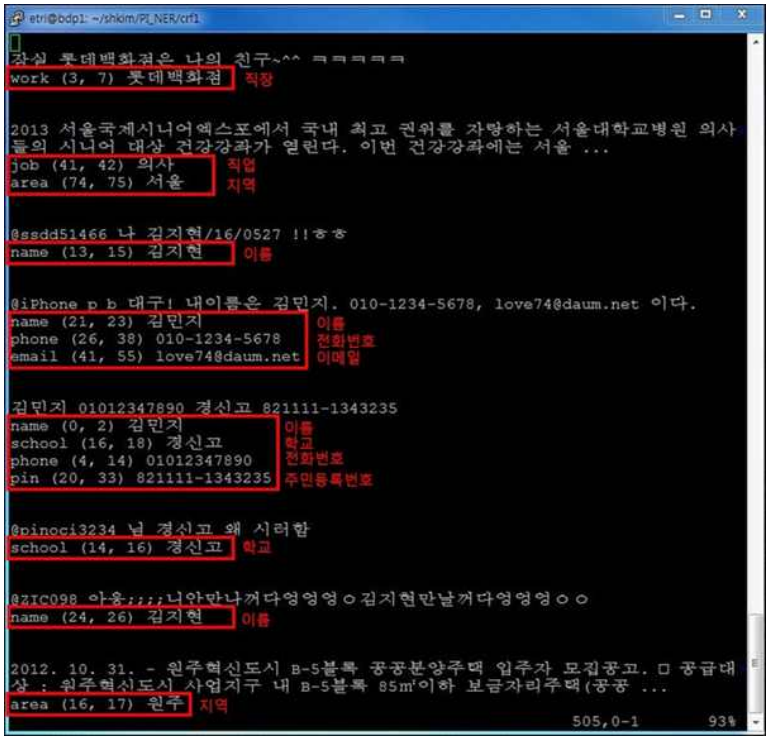
○ 개인정보 리스크 탐지

- 개인정보 8종 탐지/정규화 -> 특정성 분석
- 페이스북, 트위터 960만명의 정보 노출 현황 분석

- 정형정보 3종, 비정형정보 5종 탐지/정규화
- 단독 및 조합 정보의 k-anonymity 분석

○ 분석 방법

- SNS 서비스 개인정보 crawling (960만 계정)
- 사용자 메시지로부터 개인정보 추출 자동화
- k-anonymity 분석을 위한 개인정보 추출 및 정규화
- k-anonymity 기반의 개인 특정 위험성 분석

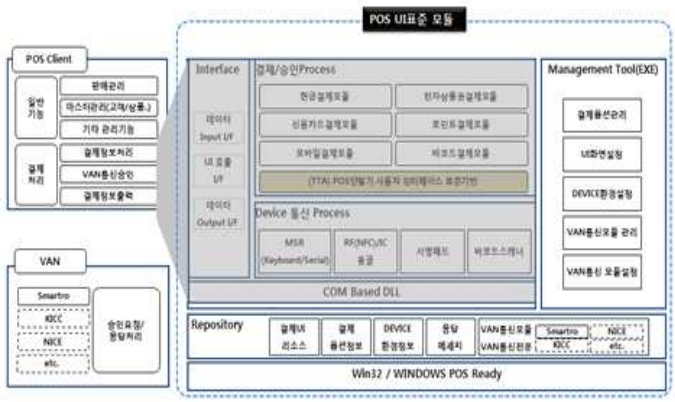


[그림 3-19] 개인정보 8종 탐지 시연 화면

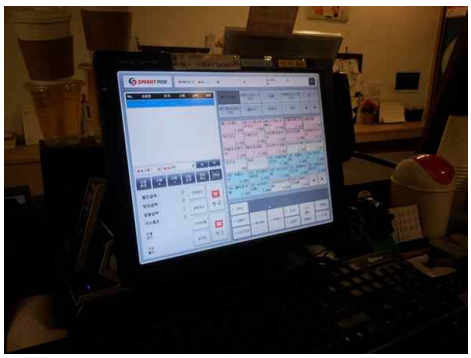
4) 표준 POS 시스템

○ 개발 내용

- 신용카드 정보, 영수증 정보를 안전하게 보호하고 유통시키기 위한 단체표준 개발 및 관련 POS 시스템 구현
- 스마트결제 단말 표준 사용자 인터페이스 모듈 개발: 모바일 신용카드, 모바일 전자 영수증 등 결제 관련한 표준 사용자 화면을 제공
- 스마트결제 단말 표준 결제모듈 인터페이스 개발: 모바일 신용카드 동글 등 주변기기와 IC거래승인을 통합지원하기 위한 인터페이스 제공



[그림 3-20] 표준 POS 시스템 구조도



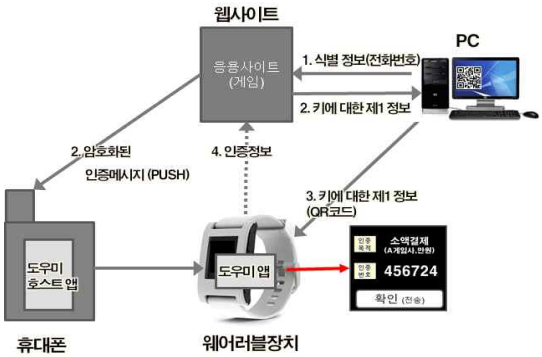
[그림 3-21] 표준 POS 설치

(2013년 10월. 서울시 서초동 미스아메리카노)

5) 웨어러블 장치 기반의 인증서비스 프로토타입

○ 개발 내용

- 웨어러블 장치를 이용하여 스마트폰이 해킹된 환경에서도 안전하게 전자서명 및 휴대폰 인증이 가능한 보안도우미 기술 구현
- 전자서명 거래원문이 조작되는 공격을 방지하기 위해, 웨어러블 장치를 통하여 거래내역을 확인하고 확인된 결과를 검증해주는 거래내역확인 기술 제공
- 본인확인, 소액결제, 2차인증 등에서 사용되는 기존 SMS 기반 휴대폰 인증 기술들이 갖는 보안 문제(인증정보 노출, 가로채기 등)를 해결하는 휴대폰 인증 기술 제공



[그림 3-22] 프로토타입 구조도

[그림 3-23] 서비스 시연

제 2 절 2차년도 연구개발 결과

1. 2차년도 연구개발 추진 일정

[표 3-3] 2차년도 연구개발 추진 일정

과제내용	추진일정 2014년 1	2	3	4	5	6	7	8	9	10	11	12	활동 책임자	연구 개발비 (천원)	참여 인력 (M/Y)
개인정보 유통 보안 시스템 기술 개발 - In-Store 개인정보 유통 보안 인터랙션 기술 개발 - In-Store 스마트결제 시스템 기술 개발 - 개인정보 유통 보안 시스템 기술 표준화	→	→	→	→	→	→	→	→	→	→	→	→	진승헌 (김수형) (장석호)	472,333 (200,000)	3.643 (1.45)
메모리해킹 피싱 공격 방지 기술 개발 - 메모리해킹 기반의 온라인 개인정보 탈취 모델 개발 - 악성코드 피싱/파밍 공격 방지 기술 개발	→	→	→	→	→	→	→	→	→	→	→	→	진승헌 (김승현)	472,333	3.643
개인정보 조합 리스크 분석 기술 개발 - 개인정보 조합식별위험 분석 기술 개발 - 개인정보 정규화 기술 - 개인정보 필터링 기술	→	→	→	→	→	→	→	→	→	→	→	→	진승헌 (최대선)	472,333	3.643
주요 Milestone 완성점에서의 수행결과	- 요구사항 정의서 - 기능 정의서 - 설계서 - 국내특허 : 4건 - 국제특허 : 2건 - 비SCI논문 : 8건 - 표준기고서 : 0건 - 기술문서 : 22건 - 기술이전 : 1.95억								- 시험절차서 - 시험결과서 - 국내특허: 1건 - 국제특허: 1건 - 비SCI논문: 3건 - 표준기고서: 2건 - 기술문서: 33건 - 기술이전: 1.2억 - SW 등록: 11건					1,617,000	12.38

2. 2차년도 연구개발 추진 실적

[표 3-2] 2차년도 연구개발 추진 실적

목 표	세 부 계 획	실 적
프라이버시 보호 모델 및 개인정보 유통 보안 요소기술 개발 (정량적 성과)	○ 특허 - 국내 특허 출원 5건 - 국제 특허 제출 3건 ○ 논문 - 비SCI 8건 - SCI 2건 ○ 표준화 - 기고서 2건 ○ 기술이전 0.7억 ○ S/W등록 3건 ○ 기술문서 50건	○ 특허 - 국내 특허 출원 5건 - 국제 특허 출원 3건 ○ 논문 - 비SCI 국제 1건 게재 - 비SCI 국내 10건 ○ 표준화 - 국내 표준안 1건 채택 - 국제 기고서 1건 채택 ○ 기술이전 3.15억 ○ S/W등록 11건 ○ 기술문서 55건
요구사항 분석 및 기능 정의	○ 요구사항 정의 ○ 기능 정의	○ 요구사항 정의서 (기술문서) - 사용자/시스템 요구사항 ○ 기능 정의서 (기술문서) - 개인정보유통보안 - 온라인 피싱 방지 - 개인정보 조합 리스크 분석 ○ 논문 - 터치사인 오프라인 전자서명 시스템 구현 - iBeacon기술 동향 및 문제점 분석 - 목표 문자열을 이용한 문자 인식 판별 방법 - 터치사인 온라인 시스템 구현 - 아이핀(i-PIN) 서비스에 대한 액티브 피싱 공격

목 표	세 부 계 획	실 적
		- 터치사인에서 인증서 관리 시스템 구현 - 관계형 데이터베이스에서 준식별자를 이용한 익명화 처리 기법 - 패스워드 없는 인증기술:FIDO - 다중 소셜 네트워크 서비스 간에 사용자 연결 방법 - 온라인 중고물품판매에 대한 개인정보노출 위협 - Device Control Protocol using Mobile Phone - [SCI Conditional Accept] Inferring Korean Residence Registration Numbers from Public Information on SNS - [SCI 제출] Undisclosed Private Attribute Inference from Facebook Profile Data ○ 기술문서 - 터치사인 기술 소개 - TTA금융보안 표준화 현황 - 거래확인 기술 - iBeacon - 터치사인 온라인 논문 - 터치사인 보안 - HFP 시나리오 - FIDO 등록 정의 값 개요 - FIDO 메타데이타 개요 - 이클립스 SVN 개발환경 가이드 - 안드로이드 SSL 구축 가이드 - FIDO 인증장치 개요 - FIDO ASM 개요 - FIDO ASM 서비스 AIDL - channel-id

목 표	세 부 계 획	실 적
		- HOBA 조사 - 보이스피싱 방지 대책 - M-PIN 조사 - 서드파티 쿠키 악용 시나리오 - 인증기술 뉴스레터-2014년 10월 - 인증기술 뉴스레터-2014년 9월 - FIDO 연합 현황 - PKCS11 라이브러리 구조 - 국내 공인인증기술의 기술적 의미 - UAF 프로토콜 소개 - 공인인증서 이슈와 현황 - 인증 R&D 로드맵 - 터치사인 인증서 관리 시스템 소개 - DB 비정상행위 탐지 논문 - 협업정보시스템에서 비정상 내부자 탐지 - SIEM 동향 - 컨텍스트 인증 - Intrusion Detection in Database - Weighted Sequence Mining - Intrusion Detection in Database - time signature - 국내 DB 접근제어 관련 기술 - ID Mapping 연구 동향 - SNS 보안 위협 및 대응 방안 - 개인정보 소유자 식별 규칙 - 트윗 문장에서 개체명 탐지 논문 연구 - 다중 소셜 네트워크 서비스 간에 사용자 연결 방법 - 의존 관계 추출 기법 논문 연구 - 익명화 처리 기법 - 국내외 인터넷 평판조회 서비스 동향 고찰 - 잊혀질 권리 관련 동향 및 전망 - 남겨질 권리 고찰

목 표	세 부 계 획	실 적
		- NBD-PWG 조사 - 건보원의 환자 표본자료 분석 - 개인정보 및 관계정보 태깅 관련 정리 - 공공데이터 포털 고찰
시스템 설계	○ 개인정보유통보안 설계 ○ 온라인 피싱 방지 설계 ○ 개인정보 조합 리스크 분석 설계	○ 개인정보유통보안 - 보안 체크인 - 핸즈프리 결제 인증 - FIDO 서버 설계 . 사용자 등록/삭제 . 인증장치 등록/인증/해지 - FIDO 클라이언트 설계 . 인증장치 등록/인증/해지 - HFP ASM 모듈 설계 . 인증장치 등록 . 사용자 인증 - 인증장치 모듈 설계 ○ 온라인 피싱 방지 - 웹브라우저 메모리 해킹 . 웹브라우저 이용 메모리 위치 확인 - 터치사인 온라인 . 전자서명 기능 . 웹브라우저 연동 ○ 개인정보 조합 리스크 분석 - 개인정보 조합 식별 위험 분석 기술 설계 . ID Mapping 알고리즘 . ID Mapping GUI 툴 - 개인정보 정규화 기술 설계 . 개인정보 세분화 . 개인정보별 정규화 처리 - 개인정보 필터링 기술 설계 . 비정형 개인정보 탐지 및 추출 . 익명화 처리 및 GUI 툴

목 표	세 부 계 획	실 적
시스템 구현	○ 개인정보유통보안 구현 ○ 온라인 피싱 방지 구현 ○ 개인정보 조합 리스크 분석 구현	○ 개인정보유통보안 - 개인정보 유통보안 인터랙션 모듈 - 개인정보 유통보안 파이도 클라이언트 모듈 - 개인정보 유통보안 파이드 서버 모듈 ○ 온라인 피싱 방지 - 웹브라우저 메모리해킹 툴킷 - 터치사인 온라인 전자서명 ○ 개인정보 리스크 탐지 - 개인정보 추출기 모듈 - 개인정보 태깅 및 익명화 모듈 - 사용자 연결 모듈 - 프로파일 정보 수집 모듈
표준화 추진	○ 국내 표준 - 표준안 채택 1건 ○ 국제 표준 - 기고서 채택 1건	○ 국내 표준안 1건 채택 - 대면거래에서의 전자서명 규격 (TTA) ○ 국제 기고서 1건 채택 - Digital Certificate and Beyond (W3C)

3. 각 기관/기업별 추진 내역

가. 스마트결제/공유를 위한 단말 인터페이스 개발

공동연구기관: (주)비씨카드

○ 연구개발 배경 및 연구목표

- 연구개발 배경 및 필요성
  - 스마트폰을 꺼내 앱을 실행하는 행위는 카드를 긁는 행위에 비해 편리성을 제공하지 못함
  - 고객은 새롭고 간편하면서도 강력한 보안을 수반하는 결제방법을 원함
  - 가맹점은 방문고객 profile을 알기 원하고, 고객은 가맹점이 자기를 알아주어 특별한 혜택을 제공받길 원함

- 연구목표
  - 스마트폰 소지만으로 비밀번호 입력 없이 결제존을 지나가면 결제완료
  - 상점에 입장하면 나를 자동 인식하여 나에게 맞는 정보를 알려 주고 결제

○ 스마트결제 서비스 흐름도

[그림 3-24] 스마트결제 서비스 흐름도

- 비콘 기반 사용자 인식 및 강력한 보안기능은 ETRI에서 담당
- 비콘 기반 간편 결제를 제공하는 POS 시스템 개발
- POS, 결제서버 인터페이스 개발

○ 연구개발 효과

- 온라인 간편결제 가입자들이 오프라인 상점에서도 동일한 서버형 결제 방법을 통해 이용할 수 있음
- BigData 분석을 통해 개인 맞춤형 마케팅정보를 전달하는 채널로 활용할 수 있음
- 긴 줄을 서지 않고 전용 출입구를 지나가는 것으로 결제 가능

4. 기술개발 결과의 유형 및 무형 성과

가. 특허

: 국내 출원 5건, 국제 출원 중 3건

1) 모바일 인증 시스템 및 방법

2) 문자 인식의 후처리 방법 및 이를 이용하는 문자 인식 장치

3) 전자 서명 제공 장치 및 방법

4) IC 카드를 인증 매체로 이용하기 위한 방법, 장치 및 시스템

5) 구역 기반의 사용자확인 시스템과 그 방법 및 구역 기반의 사용자확인 서버

6)

7)

8)

나. 프로그램

: 등록 11건

1) 개인정보 유통보안 인터랙션 모듈

- 인증 및 결제를 위한 비콘 기반 Zone인식 기능 및 체크인 관련 보안 기능

2) 개인정보 유통보안 FIDO 인증 모듈

- FIDO 표준 방식의 인증 서비스 및 개인키의 안전한 저장 관리

3) 메모리해킹 툴킷 및 시연페이지

- 금융기관 대상의 메모리해킹 툴 및 터치사인 온라인 시연페이지

4) 개인정보 유통보안 파이도 서버 모듈

- FIDO 표준 방식의 인증 서비스 및 개인키의 안전한 저장 관리

5) 데이터베이스 로그 생성

- 데이터베이스 정상 행위 탐지시스템을 실험하기 위한 데이터베이스 로그

생성

6) 데이터베이스 비정상 탐지 유저 인터페이스

- 데이터베이스에 접근하는 비정상 행위를 탐지하기 위한 시스템의 유저 인터페이스

7) 데이터베이스 비정상탐지 엔진

- 데이터베이스에 접근하는 비정상 행위를 탐지하기 위한 시스템 엔진

8) 개인정보 추출기 모듈

- 사전에 개인정보 및 관계정보에 대한 다량의 예제를 통해 학습한 학습모델을 활용하여, TXT 파일상 존재하는 개인정보를 인식하고 추출하며 그 관계를 자동으로 부여하는 프로그램

9) 개인정보 태깅 및 익명화 모듈

- TXT, HWP 등의 파일에 대해서 개인정보를 추출하고 익명화 할 수 있는 프로그램

10) 사용자 연결 모듈

- 동일한 페이스북, 트위터, 네이버 사용자를 식별하여 연결하는 프로그램

11) 프로파일 정보 수집 모듈

- 페이스북, 트위터의 사용자 프로파일 정보 및 네이버에 노출된 개인정보를 수집하여 DB에 저장하는 프로그램

다. 논문

: 국제 게재 1편, 국내 게재 10편

1) 터치사인 오프라인 전자서명 시스템 구현, 전자공학회 하계종합학술대회

2) iBeacon기술 동향 및 문제점 분석, 한국컴퓨터종합학술대회

3) 목표문자열을 이용한 문자 인식 판별 방법, 통신학회 학계종합학술대회

4) 터치사인 온라인 시스템 구현, 전자공학회 하계종합학술대회

5) 아이핀(i-PIN) 서비스에 대한 액티브 피싱 공격, 전자공학회 하계종합학술대회

6) 터치사인에서 인증서 관리 시스템 구현, 전자공학회 하계종합학술대회

7) 관계형 데이터베이스에서 준식별자를 이용한 익명화 처리 기법, 정보보호학회 하계학술대회

8) 패스워드 없는 인증기술:FIDO

9) 다중 소셜 네트워크 서비스간에 사용자 연결 방법, 정보처리학회 추계학술대회

10) 온라인 중고물품판매에 대한 개인정보 노출 위험, 정보처리학회 추계학술대회

11) Device Control Protocol using Mobile Phone, ICACT 2014

라. 국내 표준화

: TTA 표준안 채택 1건 채택

1) 대면거래에서의 전자서명 규격

- 대면거래 시에 종이 문서 대신 스마트 단말을 통해 전자적으로 개인정보를 입력하는 서비스 시스템에서 사용자의 전자서명을 거래 상대가 소지한 스마트 단말에 제공하는 시나리오와 메시지 규격을 정의함

마. 국제 표준화

: W3C 국제 기고서 채택 1건

1) Digital Certificate and Beyond 기고서

- W3C Workshop, 2014년 9월, 샌프란시스코
- 공인인증서의 사용 편의성과 보안 취약성을 개선하기 위한 일련의 기술 개발을 소개하는 기고서
- 자바스크립트 기반의 인증서 관리, NFC 기반의 인증서를 이용하여 사용자를 인증하는 터치사인 및 패스워드를 사용하지 않고 인증서를 이용하는 FIDO 기반 사용자 인증 기술 소개

[그림 3-25] W3C Workshop

2) 산업계 개방형 인증 표준 단체인 FIDO Alliance 회원가입

- FIDO Alliance는 2012년 7월 출범하여 구글, 마이크로소프트, 퀄컴, 레노보 등 IT 기업과 비자, 마스터, 페이팔 등 전세계 140 개 회원사가 참여
- 국내는 삼성전자, LG전자, 크루셜텍, SK텔레콤, ETRI등 회원사로 활동 중
- FIDO는 패스워드 대신 지문, 얼굴 등 생체인식과 보안토큰 등 강력한 인증 수단을 사용할 수 있는 인증 및 전자서명 기술
- 공인인증서 대체 기술의 표준화를 주도하여 연구결과물의 국제경쟁력 강화

[그림 3-26] FIDO Alliance 회원 가입

바. 공공/공익적 연구성과 활용 실적

1) 액티브X없는 공인인증서 보안 기술로 터치사인 제공

- 3월20일 열린 규제개혁장관회의 및 민관합동 규제개혁 점검회의에서 대통령이 "전자상거래시 공인인증서 및 액티브엑스(Active-X) 때문에 외국인이 '천송이 코트'를 살 수 없다"고 지적하며 액티브엑스 폐지 추진
- 공인인증서비스와 달리 액티브엑스를 사용하지 않는 터치사인 기술을 활용하여 공인인증서의 편의성/보안성 강화하기 위해 미래부, 한국인터넷진흥원이 준비 중인 액티브X없는 공인인증서 시범사이트에 터치사인 적용을 위한 기술 지원

[그림 3-27] 액티브X없는 터치사인

사. 기술이전

: 기술이전 5건 완료

1) 기술이전명: 터치사인
   - 21,000만원

2) 기술이전명: 스마트인증 및 개인정보 탐지 모듈
   - 10,500만원

아. 상용화 지원

1) 1실1기업 지원

- 듀얼아이 : 핸즈프리 인증 서비스 파일럿 개발 지원

  지원 건수 : 15건

- 쿠노소프트 : 지불 확인 기술 지원

  지원 건수 : 8건

- 케이사인: DB 개인정보보호 기술 지원

  지원 건수 : 7건

- 코나아이 : 터치사인 기술 지원

  지원 건수 : 4건

[그림 3-28] 1실 1기업 지원

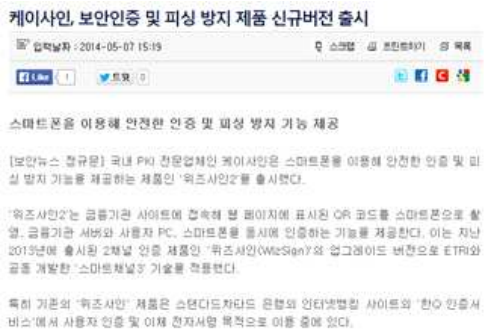
2) 비씨카드와 ZEP(Zero Effort Payment) 파일럿 서비스 (11월말~)

- 적용기술: 비콘 기반 보안 체크인 및 FIDO 강화인증 기술(ETRI), 가상카드 결제 및 개인화 서비스(비씨카드)
- 파일럿 장소: 비씨카드 사내식당 (직원대상으로 식당 이용금액을 파일럿 시스템으로 결제)
- 파일럿 목적: 핸즈프리 결제 기술을 비씨카드 영업/홍보 담당자 및 외부관계사(은행, VAN사 등)에 소개하고, 향후 서비스 상용화를 추진하기 위한 운영 경험 축적과 응용 서비스 개발에 활용

[그림 3-29] 비씨카드와 ZEP 파일럿 서비스

3) 스마트채널3 상용화

- 케이사인, 투채널 인증솔루션인 '위즈사인2' 출시
- ETRI의 '스마트채널3' 기술 적용
- 일시 : 2014년 5월 7일
- 신문 : 전자신문, 연합뉴스, 보안뉴스, 디지털 타임즈 외 다수



케이사인, 보안인증 및 피싱 방지 제품 신규버전 출시

입력날자 : 2014-05-07 15:19

스마트폰을 이용해 안전한 인증 및 피싱 방지 기능 제공

[보안뉴스 정규문] 국내 PKI 전문업체인 케이사인은 스마트폰을 이용해 안전한 인증 및 피싱 방지 기능을 제공하는 제품인 '위즈사인2'를 출시했다.

'위즈사인2'는 금융기관 사이트에 접속해 뜬 페이지에 표시된 QR 코드를 스마트폰으로 촬영, 금융기관 서버와 사용자 PC, 스마트폰을 동시에 인증하는 기능을 제공한다. 이는 지난 2013년에 출시된 2채널 인증 제품인 '위즈사인(WizSign)'의 업그레이드 버전으로 ETRI와 공동 개발한 '스마트채널3' 기술을 적용했다.

특히 기존의 '위즈사인' 제품은 스탠다드차타드 은행의 인터넷뱅킹 사이트와 '한G 인증서 비스'에서 사용자 인증 및 이체 전자서명 목적으로 이용 중에 있다.

[그림 3-30] 스마트채널3 상용화

4) 개인정보 리스크 분석 기술

- 프라이버시 스캐닝 솔루션 업체와 개발 단계에서 협력하여 기술이전 및 상용화 추진
  - 종래에 주민번호 등 정형 정보만 탐지하는 수준에 이름, 지역, 직장 등 비정형 정보 탐지 기능 추가 예정

- 공공 데이터 개방 전 프라이버시 필터링 적용 협의
  - 정부 3.0 공공데이터 개방: 2015년 1억건, 2017년 7.7억건 예정
  - 식별성, 재식별성에 대한 사전, 사후 관리 필요
  - 안행부, NIA 등 주무기관과 프라이버시 필터링 기술 적용 협의 (14년 5월)

[그림 3-31] 개인정보 리스크 분석 기술

자. 전시회 참가

1) 세계 보안 엑스포 2014(SECON 2014)

- 2014.3.12.~3.14, KINTEX
- 국내외 총 320여 개 기고나이 참가한 대규모 보안 전시회 참가
- 정부/유관기관/업체 등 관계자에게 스마트인증(터치사인, 스마트채널) 기술 시연 및 소개

[그림 3-32] 세계 보안 엑스포 2014

2) 미래창조과학부 R&D 성과확산대전

- 2014.11.05.~11.07, KINTEX
- 산학연 기술교류 및 사업화 설명회에서 스마트인증 기술 소개
- R&D 결과의 기술이전 협약 체결(한국스마트ID) 등

[그림 3-33] R&D 성과확산대전

차. 보도 자료

1) 터치사인 기술 개발

- 터치 사인 기술
  - 스마트폰에 카드를 터치하여 전자서명/로그인 기능
  - NFC를 이용한 전자서명 기술
  - 공인인증서 차세대 인증기술
- 일시 : 2014년 1월 14일
- 방송 : YTN 사이언스, 연합뉴스 TV
- 신문 : 중앙일보, 경향신문, 전자신문, 디지털 타임즈 외 다수

[그림 3-34] 터치사인 보도 자료

2) 스마트채널3 기술 개발

- 스마트채널3 기술
  - 안전한 전자정부·금융 서비스 활용 '스마트채널 3' 개발
  - 스마트폰 카메라로 QR코드 및 웹 주소인식, 피싱 확인
  - 암호키 관리·보안문제 해결한 보안쿠키로 사용자PC 인증
- 일시 : 2014년 1월 23일
- 신문 : 전자신문, 연합뉴스, 보안뉴스, 디지털 타임즈 외 다수

ETRI, 스마트폰으로 피싱 방지한다

입력날자 : 2014-01-23 10:06 스크랩 프린트하기 목록

Like 3 트윗 2

안전한 전자정부·금융 서비스 활용 '스마트채널 3' 개발

[보안뉴스 김태형] 금융거래가 컴퓨터를 이용하는 것이 보편화 되면서 악의적인 목적으로 개인정보 침해는 물론 금융사고도 빈발하고 있다. 이에 간단히 스마트폰을 이용해 웹 브라우저 주소 창을 확인하고 로그인하는 기술이 국내 연구진에 의해 개발되어 안심할 수 있는 금융거래가 가능케 될 전망이다.

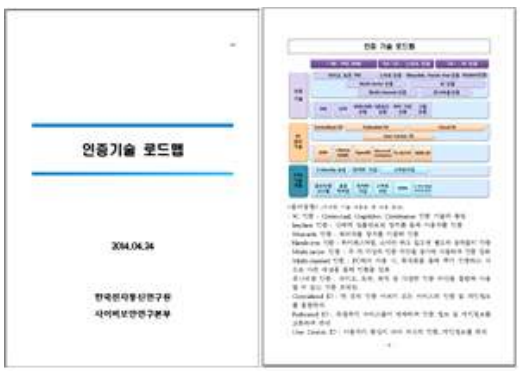
ETRI(한국전자통신연구원, 원장 김흥남)는 스마트폰을 이용한 안전한 인증 및 피싱 방지 기능을 제공하는 '스마트채널3' 기술을 개발했다고 23일 밝혔다.

[그림 3-35] 스마트채널3 보도 자료

카. 기술 동향 분석

1) 인증기술 로드맵

- 차세대 인증 기술 및 ETRI 보유 인증 기술 로드맵 작성
- 4월 24일 미래창조과학부 정보보호 정책과 보고



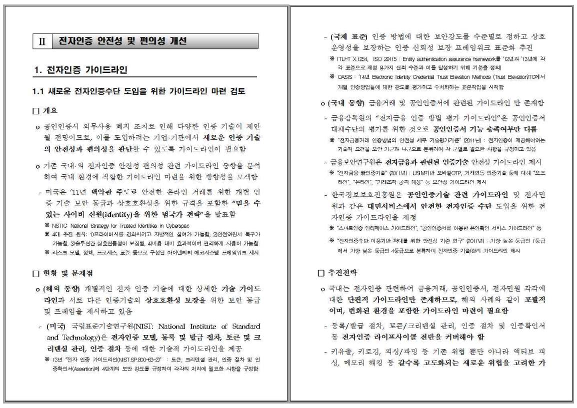
인증기술 로드맵

2014.04.24

[그림 3-36] 인증기술 로드맵

2) 전자인증발전방향

- 전자인증 안전성 및 편의성 개선 방안 도출
- 차세대 전자인증 기술 개발
- 10월 미래창조과학부 정보보호 정책과 보고



II 전자인증 안전성 및 편의성 개선

1. 전자인증 가이드라인

1.1 새로운 전자인증수단 도입을 위한 가이드라인 마련 검토

□ 개요

o 공인인증서 의무사용 폐지 조치로 인해 다양한 인증 기술이 제안될 전망이므로, 이를 도입하려는 기업·기관에서 **새로운 인증 기술의 안전성과 편의성을 판단**할 수 있도록 가이드라인이 필요함

o 기존 국내·외 전자인증 안전성 편의성 관련 가이드라인 동향을 분석하여 국내 환경에 적합한 가이드라인 마련을 위한 방향성을 모색함

- 미국은 '11년 **백악관 주도로** 안전한 온라인 거래를 위한 개별 인증 기술 보안 등급과 상호호환성을 위한 규격을 포함한 **"믿을 수 있는 사이버 신원(identity)을 위한 범국가 전략"**을 발표함

※ NSTIC National Strategy for Trusted Identities in Cyberspac

※ 4대 추진 원칙: 1)프라이버시를 강화시키고 자발적인 참여가 가능함, 2)안전하면서 복구가 가능함, 3)솔루션간 상호연동성이 보장됨, 4)비용 대비 효과적이며 편리하게 사용이 가능함

※ 리스크 모델, 정책, 프로세스, 표준 등으로 구성된 아이덴티티 에코시스템 프레임워크 제시

□ 현황 및 문제점

o **(해외 동향)** 개별적인 전자 인증 기술에 대한 상세한 **기술 가이드라인**과 서로 다른 인증기술의 **상호호환성 보장**을 위한 보안 등급 및 프레임을 제시하고 있음

- **(미국)** 국립표준기술연구원(NIST: National Institute of Standard and Technology)은 **전자인증 모델, 등록 및 발급 절차, 토큰 및 크리덴셜 관리, 인증 절차** 등에 대한 기술적 가이드라인을 제공

※ 13년 "전자 인증 가이드라인(NIST.SP.800-63-2)" : 토큰, 크리덴셜 관리, 인증 절차 및 인증확인서(Assertion)에 4단계의 보안 강도를 규정하여 각각의 처리에 필요한 사항을 규정함

- **(국제 표준)** 인증 방법에 대한 보안강도를 수준별로 정하고 상호 운영성을 보장하는 인증 신뢰성 보장 프레임워크 표준화 추진

※ ITU-T X.1254, ISO 29115 : Entity authentication assurance framework를 '12년과 '13년에 각각 표준으로 제정 (4가지 신뢰 수준과 이를 달성하기 위해 기준을 정의)

※ OASIS : '14년 Electronic Identity Credential Trust Elevation Methods (Trust Elevation)TC에서 개별 인증방법들에 대한 강도를 평가하고 수치화하는 표준작업을 시작함

o **(국내 동향)** 금융거래 및 공인인증서에 관련된 가이드라인 만 존재함

- 금융감독원의 "전자금융 인증 방법 평가 가이드라인"은 공인인증서 대체수단의 평가를 위한 것으로 **공인인증서 기능 충족여부만 다룸**

※ "전자금융거래 인증방법의 안전성 세부 기술평가기준" (2011년) : 전자인증이 제공해야하는 기술적 요건을 보안 가군과 나군으로 분류하여 각 군별로 필요한 사항을 규정하고 있음

- 금융보안연구원은 **전자금융과 관련된 인증기술** 안전성 가이드라인 제시

※ "전자금융 新인증기술" (2011년) : USIM기반 모바일OTP, 거래연동 인증기술 등에 대해 "오프라인", "온라인", "거래조작 공격 대응" 등 보안성 가이드라인 제시

- 한국정보보호진흥원은 **공인인증기술 관련 가이드라인** 및 전자민원과 같은 **대민서비스에서 안전한 전자인증 수단** 도입을 위한 전자인증 가이드라인을 제정

※ "스마트인증 인터페이스 가이드라인", "공인인증서를 이용한 본인확인 서비스 가이드라인" 등

※ "전자인증수단 이용기반 확대를 위한 안전성 기준 연구" (2011년) : 가장 높은 등급인 1등급에서 가장 낮은 등급인 4등급으로 분류하여 전자인증 기술/관리 가이드라인 제시

□ 추진전략

o 국내는 전자인증 관련하여 금융거래, 공인인증서, 전자민원 각각에 대한 **단편적 가이드라인만 존재하므로,** 해외 사례와 같이 **포괄적이며, 변화된 환경을 포함한 가이드라인 마련이 필요함**

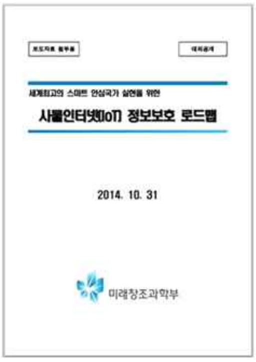
- 등록/발급 절차, 토큰/크리덴셜 관리, 인증 절차 및 인증확인서 등 **전자인증 라이프사이클 전반을 커버해야 함**

- 키유출, 키로깅, 피싱/파밍 등 기존 위협 뿐만 아니라 액티브 피싱, 메모리 해킹 등 **갈수록 고도화되는 새로운 위협을 고려한 가**

[그림 3-37] 전자인증발전방향

3) IoT 정보보호 계획

- 사물인터넷 정보보호 로드맵 작성
- 미래창조과학부에서 10월 31일 관계부처 차관회의에서 보고
- IoT 서비스 플랫폼 중 스마트 인증, IoT 프라이버시 보호를 위한 보안 핵심 기술 제안



세계최고의 스마트 안심국가 실현을 위한

사물인터넷(IoT) 정보보호 로드맵

2014. 10. 31

미래창조과학부

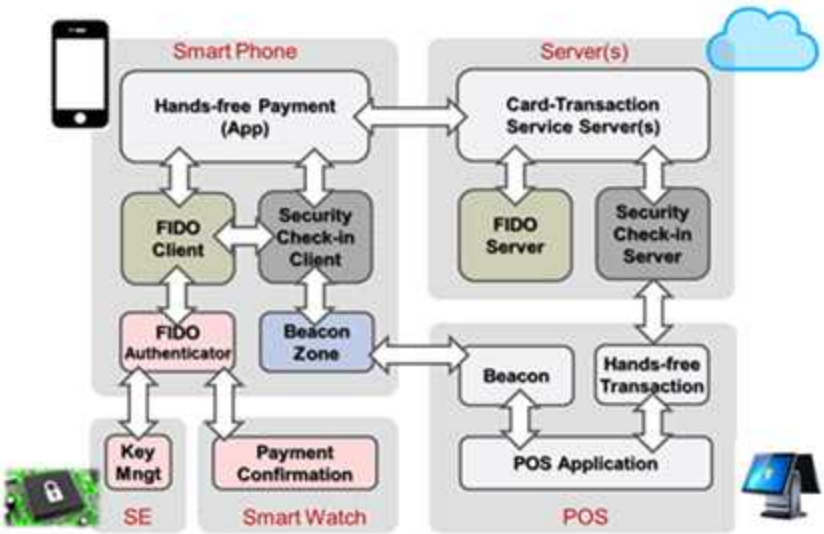
[그림 3-38] IoT 정보보호 계획

타. 시스템 개발

1) 개인정보 유통 보안 시스템 기술

○ 핸즈프리 결제 시스템

- 개발 내용
  - 사용자가 상점 방문 시 비컨을 통해 구성된 체크인 Zone을 사용자 스마트폰이 인식하여 사용자 식별정보 노출 없는 안전한 체크인을 수행하고, 사용자가 POS 시스템 앞 5m 이내의 결제 Zone에 들어서면 사용자 맞춤형 정보가 자동 제공되며, 실물 카드를 소지하지 않아도 사용자 의사만으로 안전한 결제 서비스를 제공하는 핸즈프리 결제 시스템 개발
  - 개발된 보안 기술은 사용자 식별정보 수집 및 재사용 공격 등에 대응하며, 결제 의사가 있는 오프라인 매장 내 사용자를 자동 인식하며, 결제 시에는 국제표준 기반의 FIDO 기술을 활용한 인증 강화 기술을 적용하여 기존 결제 서비스 이상의 강력한 보안을 제공



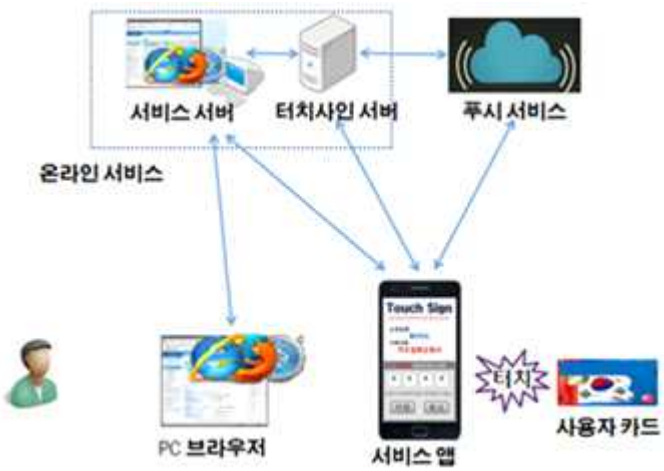
[그림 3-39] 핸즈프리 결제 시스템 구조도

[그림 3-40] 핸즈프리 결제 시스템 시연 화면

2) 메모리해킹 피싱 공격 방지 기술

○ 터치사인-온라인

- 개발 내용
  - PC의 웹브라우저를 사용하여 웹서비스를 이용할 때 공인인증서를 이용한 전자서명 및 로그인 작업을 사용자 휴대폰에서 수행
  - 사용자 휴대폰 정보를 입력하여 전자서명을 요청하고 휴대폰에서 금융카드를 터치하여 전자서명결과 또는 본인확인 정보를 서버에 제공



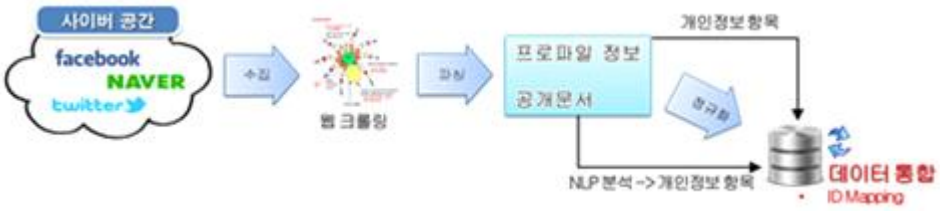
[그림 3-41] 터치사인 온라인 개념도

[그림 3-42] 터치사인 온라인 시연 화면

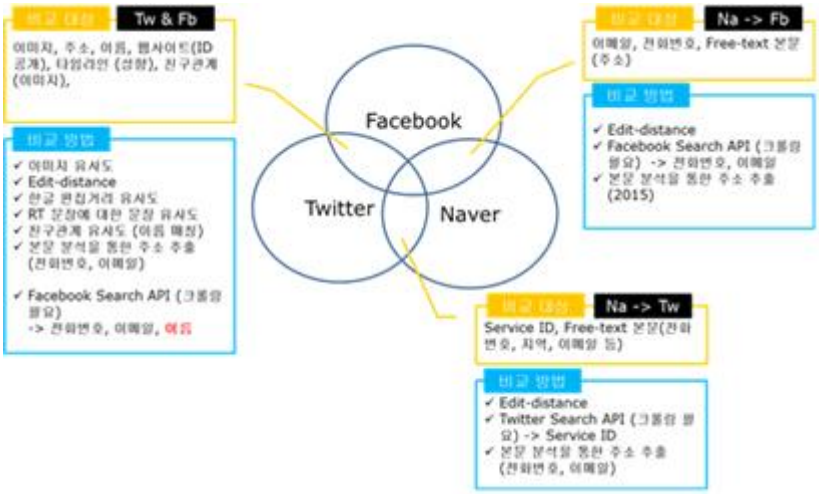
3) 개인정보 조합 리스크 분석 기술 개발

○ 개인정보 조합식별위험 분석 기술

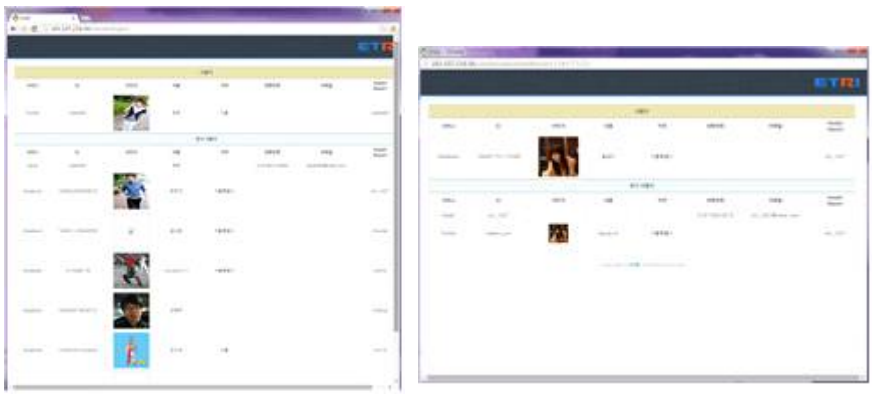
- 개발 내용
  - 공공 데이터 등 집적 데이터 및 SNS/웹사이트 등의 단문 데이터에서 개인정보를 추출하고, 해당 개인정보의 주체를 식별하여, 주체별 개인정보를 연결/조합을 통해 위험도를 제시
  - FB-TW-NA 3개 사이트 ID Mapping



[그림 3-43] 비정형 개인정보 탐지 및 조합 리스크 분석 시스템 개념도



[그림 3-44] ID Mapping 대상 및 연결 항목 예시



[그림 3-45] 개인정보 조합 식별 결과 화면 예시

○ 개인정보 정규화 기술

- 개발 내용
  - 개인정보를 13종으로 세분화하여, 각각의 개인정보별 특성을 감안하여 비교 가능하도록 정규화하는 룰 설정 및 코드화 기술

개인정보 개체명 태그 2014-09-30

대분류	중분류	소분류	AT_TYPE	정의	비고
PS (개인 이름 정보)	PS	PS_NAME	101	사람 이름(일반인)	
LC (장소 개념)	LC	LC_ADDRESS	201	주소(특별시, 광역시, 도, 시, 군, 구, 읍, 면, 동 + 번지/도로명 + 아파트/건물명 + 호수)	
		LC_PLACE	202	장소(산/강/섬, 온천, 해변, 관광지+해안, 목포, 계곡, 동굴)	(지명적으로 생성된 장소) 사람들이 모이는 곳
		LC_FACILITY	203	건물(지하철/기차역, 공항, 버스터미널, IC, 시장, 정류장, 단지, 항구, 건축물, 다리, 둥대, 문화재, 운동장, 식물원, 수목원, 정원, 공원, 세트장, 공장, 테마파크, 놀원/놀장, 발전소, 공연장) + 기관명(기업명/직장명/기관명), 백화점, 마트, 박물관, 호텔, 모텔, 원룸, 펜션, 콘도, 리조트	(인공적으로 만들어진 곳) 사람들이 모이는 곳 -->LC_FACILITY와 OG_OTHER 통합
OG (기관명 개념)		OG_SCHOOL	301	학교(출신학교, 초/중/고/대)	
PI (Personal Info)	PI_JOB	PI_JOB	401	직업 명칭	
		PI_POSITION	402	직위 명칭	
		PI_ID	403	주민등록번호	여권번호, 운전면허번호, 군번 등은 현재 미지정
		PI_CAR	404	자동차 번호판	
	PI_PHONE	PI_PHONE	405	전화번호	휴대폰과 전화번호를 하나로 통합
		PI_EMAIL	407	이메일 주소	
		PI_AGE	408	나이	
DT	DT	DT_DATE	501	날짜(년/월/일)	

[그림 3-46] 비정형 개인정보 태그 리스트

○ 개인정보 필터링 기술

- 개발 내용

  - TXT, HWP 파일의 개인정보를 탐지하여, 사용자 선택에 따라 마스킹

제 3 절 3차년도 연구개발 결과

1. 3차년도 연구개발 추진 일정

[표 3-5] 3차년도 연구개발 추진 일정

과제내용	추진일정 2014년 1	2	3	4	5	6	7	8	9	10	11	12	활동 책임자	연구 개발비 (천원)	참여 인력 (M/Y)
개인정보 (ID, 인증정보, 결제정보) 유통 보안 응용 서비스 테스트베드 개발 - 개인정보 유통 보안 응용서비스 프로토타입 개발 - In-Store 스마트결제 응용서비스 테스트베드 개발 - 개인정보 유통 보안 응용 기술 표준화	→	→	→	→	→	→	→	→	→	→	→	→	진승헌 (김수형) (성기윤)	460,281 (200,000)	3.45 (1.74)
개인정보 큐레이션 기술 개발 - 오프라인 피싱 방지 기술 개발 - 개인정보 큐레이션 기술 개발			→	→	→	→	→	→	→	→	→	→	진승헌 (김승현)	460,281	3.45
개인정보 추론 리스크 분석 기술 개발 - 개인정보 추론 탐지 리스크 분석 기술 개발 - 개인정보 이상 접근행위 탐지 프로토타입			→	→	→	→	→	→	→	→	→	→	진승헌 (최대선) (김수형)	460,281	3.45
주요 Milestone 완성점에서의 수행결과	- 요구사항 정의서 - 기능 정의서 - 설계서 - 국내특허 : 3건 - 국제특허 : 2건 - 비SCI논문 : 7건 - SCI논문: 3건 - 표준기고서 : 0건 - 기술문서 : 13건 - 기술이전 : 8.63억								- 시험절차서 - 시험결과서 - 비SCI논문: 1건 - SCI논문: 1건 - 표준기고서: 3건 - 기술문서: 17건 - 기술이전: 2.60억 - SW 등록: 4건					1,580,843	12.09

2. 3차년도 연구개발 추진 실적

[표 3-6] 3차년도 연구개발 추진 실적

목 표	세 부 계 획	실 적
프라이버시 보호 모델 및 개인정보 유통 보안 요소기술 개발 (정량적 성과)	○ 특허 - 국내 특허 출원 5건 - 국제 특허 출원 3건 ○ 논문 - 비SCI 8건 - SCI 2건 ○ 표준화 - 기고서 2건 ○ 기술이전 1억 ○ S/W등록 3건 ○ 기술문서 50건	○ 특허 - 국내 특허 출원 3건 - 국내 특허 출원중 1건 - 국제 특허 출원 2건 - 국제 특허 출원중 1건 ○ 논문 - 비SCI 8건 - SCI 3건 - SCIE 1건 ○ 표준화 - 기고서 3건 ○ 기술이전 11.23억 ○ S/W등록 4건 ○ 기술문서 30건
요구사항 분석 및 기능 정의	○ 요구사항 정의 ○ 기능 정의	○ 요구사항 정의서 (기술문서) - 사용자/시스템 요구사항 ○ 기능 정의서 (기술문서) - 개인정보 유통보안 - 개인정보 큐레이션 - 개인정보 추론 리스크 분석 ○ 논문 - FIDO UAF 1.0 서버 구현 - 일반화와 데이터삽입을 이용한 익명화 처리 기법 - The privacy analysis of online trade market - Effects of Contextual Properties on

목 표	세 부 계 획	실 적
		Users' Privacy Preferences in Mobile Computing Environments - Accurate Indoor Proximity Zone Detection Based on Time Window and Frequency with Bluetooth Low Energy - 핀테크 기술 및 보안 동향 - 자바스크립트 변조를 이용한 국내 인터넷 뱅킹 키보드 암호화 모듈 우회 공격 - 관계형 데이터베이스에서 데이터 그룹화를 이용한 익명화 처리 기법 - Estimating Korean Residence Registration Numbers from Public Information on SNS - Short Dynamic Group Signature Scheme Supporting Controllable Linkability - Customer Data Scanner for Hands-Free Mobile Payment - New Efficient Batch Verification for an Identity-Based Signature Scheme ○ 기술문서 - FIDO 클라이언트 설계서 - FIDO 서버 설계서 - RP 클라이언트 설계서 - FIDO 1.0 ASM 인증장치 등록 - FIDO 1.0 ASM 인증 - FIDO 1.0 ASM 인증장치 해지 - FIDO 1.0 ASM 정보조회 - FIDO UAF 1.0 서버 구현 - FIDO Server 관리자 GUI 설계 - FIDO Server 설계 및 구동 방법

목 표	세 부 계 획	실 적
		- FIDO 서버 기술 교육 - GnuTLS 설치 및 테스트 - 프라이버시보호를 위한 전자서명 위임구조 1 - 위임서명 설계원리 - 프라이버시보호를 위한 전자서명 위임구조 2 - ID기반서명 설계원리 - 인증기술뉴스레터-2015년5월 1호 - 인증기술뉴스레터-2015년5월 2호 - 인증기술뉴스레터-2015년6월 1호 - 인증기술뉴스레터-2015년6월 2호 - 인증기술뉴스레터-2015년7월 1호 - 인증기술뉴스레터-2015년7월 2호 - 인증기술뉴스레터-2015년8월 1호 - 인증기술뉴스레터-2015년8월 2호 - 인증기술뉴스레터-2015년9월 1호 - 인증기술뉴스레터-2015년9월 2호
시스템 설계	○ 개인정보 유통보안 설계 ○ 개인정보 큐레이션 설계 ○ 개인정보 추론 리스크 분석 설계	○ 개인정보 유통보안 - 개인정보 유통보안 응용 서비스 . FIDO 서버 . FIDO 클라이언트 . FIDO 인증장치 ○ 개인정보 큐레이션 - 오프라인 피싱 방지 . 악성 BLE 비콘 탐지 - 개인정보 큐레이션 . 개인정보 접근 모니터링 . 사용자 정책 관리 . 실시간 개인정보 접근 제어 ○ 개인정보 추론 리스크 분석 - 개인정보 추론 리스크 분석 . 개인정보 추론 리스크 분석 . 비정형 개인정보 탐지 기술 고도화 - 개인정보 이상접근 탐지

목 표	세 부 계 획	실 적
		. 쿼리 정보 조회 . 관리자 규칙 관리 . 이상 행위 판단
시스템 구현	○ 개인정보 유통보안 구현 ○ 개인정보 큐레이션 구현 ○ 개인정보 추론 리스크 분석 구현	○ 개인정보유통보안 - FIDO 인증 기술 . FIDO 서버 . FIDO 클라이언트 . FIDO 인증장치 ○ 개인정보 큐레이션 - 악성 BLE 비콘 탐지 기술 . Relay attack 방지를 위한 악성 비콘 탐지 . 패킷 전송 지연을 파악하는 RS 보안 프로토콜 - 개인정보 큐레이션 시스템 . 실시간 개인정보 접근 제어 . 개인정보 접근 모니터링 . 사용자 정책 관리 ○ 개인정보 추론 리스크 분석 - 개인정보 추론 리스크 분석 . 공개 정보 조합/연결 . 비정형 개인정보 추론 - 개인정보 이상 접근 탐지 . 사용자별 SQL 쿼리 분석을 통한 기계학습 분석 . 사용자 접근 패턴 분석 . 규칙 기반 이상행위 탐지
표준화 추진	○ 기고서 2건	○ 국내 표준안 3건 채택 - FIDO -제11부- 용어 해설 (TTA) - FIDO -제10부- 보안 참조 (TTA) - FIDO AppID와 Facet 규격 v1.0 (TTA)

3. 각 기관/기업별 추진 내역

가. In-Store 스마트결제 응용서비스 테스트베드 개발

공동연구기관: (주)비씨카드

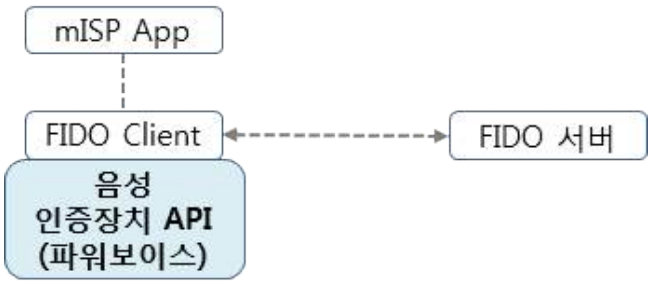
○ 연구개발 배경 및 연구목표

- 연구개발 배경 및 필요성
  - 스마트폰을 통한 간편결제 수행 시 비밀번호 입력의 경우 해당 사이트마다 다른 규칙에 따라 비밀번호를 기억하기가 쉽지 않은 불편한 점이 있음
  - 화자(Voice) 인증 등 생체정보를 이용하여 편리하게 인증하면서도 보안이 보장되는 결제방법의 적용이 필요

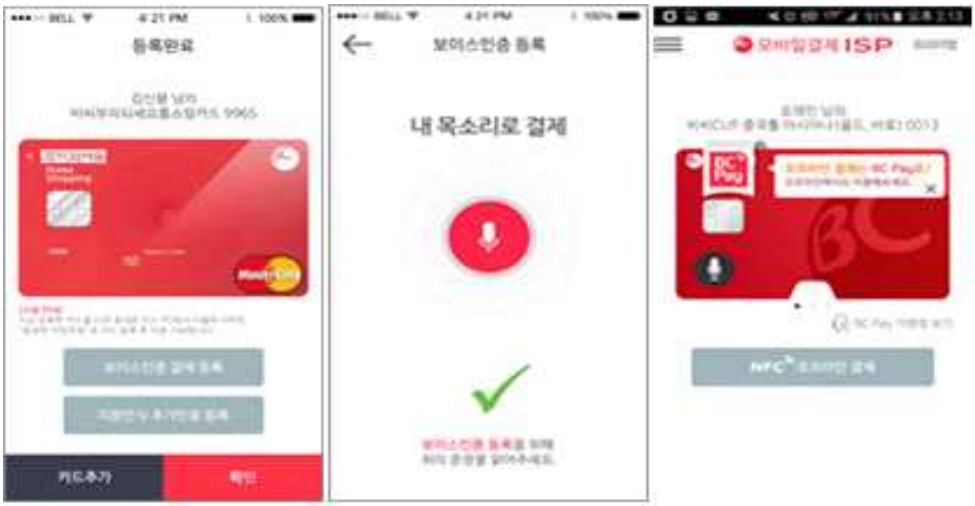
- 연구목표
  - 스마트폰에 특정 문구를 말함으로써 사용자 인증을 하고 결제 수행

○ 서비스 구성 및 흐름도

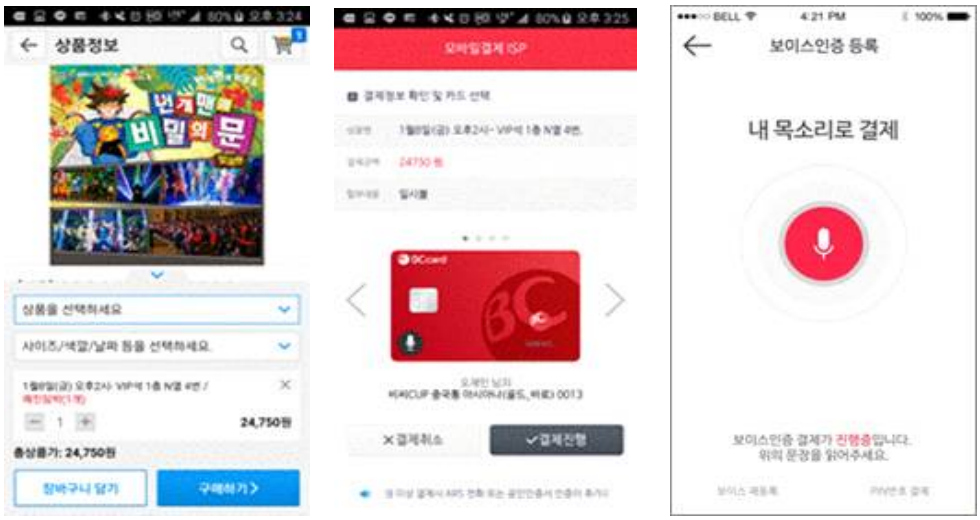
- FIDO Client, FIDO 서버, FIDO 인증장치 개발은 ETRI에서 담당
- mISP App 개발, 화자 인증 API 개발, 시스템 테스트베드 구축 및 필드 테스트는 비씨카드에서 담당



[그림 3-47] 화자(Voice) 인증 시스템 구성도



[그림 3-48] 사용자 화자 등록



[그림 3-49] 화자인증 결제

○ 연구개발 효과

- 일반 사용자 입장에서 생체정보를 통해 쉽고 안전하게 인증하고 결제할 수 있는 수단 확보

- FIDO 기반의 화자인증 서비스 적용으로 핀테크 분야 업계 리더십 확보(BC 카드는 FIDO Alliance Sponsor 지위에 있으며, Board Member 승급 추진 예정임)
- FIDO 기반의 신규 인증 서비스 추가를 통한 생체인증 포트폴리오 강화 및 이를 통한 인증 영역 확대로 향후 신규 수익원 확보 기대

4. 기술개발 결과의 유형 및 무형 성과

가. 특허

: 국내 출원 3건, 국내 출원 중 1건, 국제 출원 2건, 국제 출원 중 1건

1)

2)

3)

4)

5) Apparatus and method for providing digital signature

6) Zone-based user verification server, system, and method therof

7)

나. 프로그램

: 등록 4건

1) 개인정보 큐레이션 플랫폼

- 안드로이드 앱을 모니터링하여 개인정보 접근시 사용자가 앱 권한 제어

2) 비콘기반 근접감지 시스템

- 비콘 신호를 이용하여 스마트폰 기반의 사용자 접근을 감지하는 시스템
- 사용자의 움직임을 실시간으로 모니터링하고 움직임에 대한 시간과 위치 정보를 기반으로 특정 행위를 탐지하여 알람

3) 데이터베이스 이상행위 탐지 서버 사용자 인터페이스

- 데이터베이스 이상행위 탐지 서버의 사용자 인터페이스
- 인터페이스를 이용하여 데이터베이스에서 발생하는 쿼리를 실시간으로 확인
- 실시간 이상행위 분석 화면
- 데이터베이스의 접근 패턴 확인

4) 데이터베이스 이상행위 탐지 서버

- 데이터베이스에서 발생하는 이상 행위를 탐지하는 서버
- SQL-Injection 쿼리, Bulk 쿼리, 접근하지 않던 방식(시간, IP), 접근하지 않던 테이블 등을 이상행위로 판단
- 기계학습 및 통계를 이용한 이상행위 분석

다. 논문

: SCI 3건, SCIE 1건, 국제 게재 3편, 국내 게재 5편

1) FIDO UAF 1.0 서버 구현, 한국정보처리학회 추계학술대회
2) 일반화와 데이터삽입을 이용한 익명화 처리 기법, 한국정보처리학회 추계학술대회
3) The privacy analysis of online trade market, International Conference on Social Science and Psychology
4) Effects of Contextual Properties on Users' Privacy Preferences in Mobile Computing Environments, The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications
5) Accurate Indoor Proximity Zone Detection Based on Time Window and Frequency with Bluetooth Low Energy, The 12th International conference on Mobile Systems and Pervasive Computing
6) 핀테크 기술 및 보안 동향, 전자통신동향분석
7) 자바스크립트 변조를 이용한 국내 인터넷 뱅킹 키보드 암호화 모듈 우회 공격, 한국정보보호학회 논문지
8) 관계형 데이터베이스에서 데이터 그룹화를 이용한 익명화 처리 기법, 한국정보보호학회 논문지
9) Estimating Korean Residence Registration Numbers from Public

Information on SNS, IEICE Transaction on Communications (SCI)

10) Short Dynamic Group Signature Scheme Supporting Controllable Linkability, IEEE Transaction on Information Forensics and Security (SCI)

11) Customer Data Scanner for Hands-Free Mobile Payment, IEICE Transaction on Communications (SCI)

12) New Efficient Batch Verification for an Identity-Based Signature Scheme, Security and Communication Networks (SCIE)

라. 국내 표준화

: TTA 표준안 채택 3건 채택

1) FIDO -제9부- AppID와 Facet 규격 v1.0

- 본 표준은 유니버셜 인증 프레임워크 (FIDO UAF)의 핵심 키워드인 AppID와 FacetID에 대해서 정의함

2) FIDO -제10부- 보안 참조

- 본 표준은 유니버셜 인증 프레임워크 (FIDO UAF)와 유니버셜 2nd 팩터 (FIDO U2F)에 대한 보안 목표 및 여러 가지 보안 위험에 대한 분석 내용을 기술함

3) FIDO -제11부- 용어 해설

- 본 표준은 유니버셜 인증 프레임워크 (FIDO UAF)에서 다루어지는 기술 용어들을 정의함

마. 국제 표준화

1) 산업계 개방형 인증 표준 단체인 FIDO Alliance 회원가입 연장

- FIDO Alliance는 2012년 7월 출범하여 구글, 마이크로소프트, 퀄컴, 레노

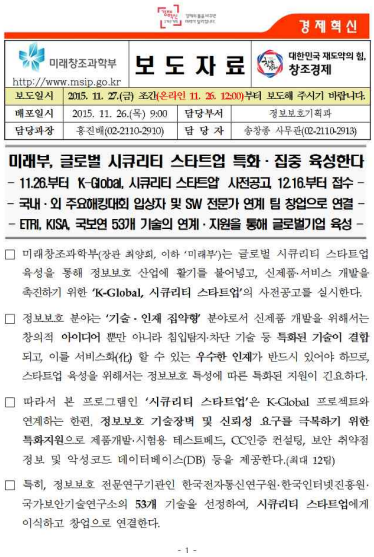
보 등 IT 기업과 비자, 마스터, 페이팔 등 전세계 240 여개 회원사가 참여

- 국내는 삼성전자, LG전자, 크루셜텍, SK텔레콤, ETRI등 회원사로 활동 중
- FIDO는 패스워드 대신 지문, 얼굴 등 생체인식과 보안토큰 등 강력한 인증 수단을 사용할 수 있는 인증 및 전자서명 기술
- ETRI는 공인인증서 대체 수단으로 FIDO 기술을 지속적으로 개발하기 위해 FIDO에 Sponsor로 가입을 연장

바. 공공/공익적 연구성과 활용 실적

1) “K-Global, 시큐리티 스타트업” 정책 참여

- 2015년 5월, 국내 주요 R&D 기관을 통해 개발된 정보보호 기술의 민간 활용 활성화 및 기술기반의 스타트업 창업 지원을 위한 지원체계 수립을 목적으로 시작된 “K-Global, 시큐리티 스타트업”에 참여
- 2015년 12월까지 FIDO 인증 기술 등 다양한 기술 제공 및 스타트업 지원 방안 마련



경제혁신

미래창조과학부 http://www.msip.go.kr

보 도 자 료

대한민국 재도약의 힘, 창조경제

보도일시	2015. 11. 27.(금) 조간(온라인 11. 26. 12:00)부터 보도해 주시기 바랍니다.		
배포일시	2015. 11. 26.(목) 9:00	담당부서	정보보호기획과
담당과장	홍진배(02-2110-2910)	담 당 자	송창종 사무관(02-2110-2913)

미래부, 글로벌 시큐리티 스타트업 특화·집중 육성한다

- 11.26부터 K-Global 시큐리티 스타트업 사전공고, 12.16부터 접수 -

- 국내·외 주요해킹대회 입상자 및 SW 전문가 연계 팀 창업으로 연결 -

- ETRI, KISA, 국보연 53개 기술의 연계·지원을 통해 글로벌기업 육성 -

□ 미래창조과학부(장관 최양희, 이하 '미래부')는 글로벌 시큐리티 스타트업 육성을 통해 정보보호 산업에 활기를 불어넣고, 신제품·서비스 개발을 촉진하기 위한 **'K-Global, 시큐리티 스타트업'**의 사전공고를 실시한다.

□ 정보보호 분야는 **'기술·인재 집약형'** 분야로서 신제품 개발을 위해서는 창의적 **아이디어** 뿐만 아니라 침입탐지·차단 기술 등 **특화된 기술이 결합**되고, 이를 서비스화(化) 할 수 있는 **우수한 인재**가 반드시 있어야 하므로, 스타트업 육성을 위해서는 정보보호 특성에 따른 특화된 지원이 긴요하다.

□ 따라서 본 프로그램인 **'시큐리티 스타트업'**은 K-Global 프로젝트와 연계하는 한편, **정보보호 기술장벽 및 신뢰성 요구를 극복하기 위한 특화지원**으로 제품개발·시험용 테스트베드, CC인증 컨설팅, 보안 취약점 정보 및 악성코드 데이터베이스(DB) 등을 제공한다.(최대 12월)

□ 특히, 정보보호 전문연구기관인 한국전자통신연구원·한국인터넷진흥원·국가보안기술연구소의 **53개** 기술을 선정하여, **시큐리티 스타트업**에게 이식하고 창업으로 연결한다.

- 1 -

[그림 3-50] K-Global, 시큐리티 스마트업 보도자료

사. 기술이전

: 기술이전 16건 완료

1) 기술이전명: 오프라인 간편결제 및 간편인증 기술

- 109,300만원

2) 기술이전명: 비정상 DB 쿼리 탐지 기술

- 3,000만원

아. 상용화 지원

1) 1실1기업 지원

- 듀얼아이 : 핀테크 관련 기술 자문 등
  지원 건수 : 4건
- 케이사인: 비정상 행위 탐지 알고리즘 지원 등
  지원 건수 : 1건

2) 상용화 현장 지원

- 지원기관: 비씨카드 (2건) - 음성인식 기술을 적용한 FIDO 인증장치를 이용하여 모바일 결제 솔루션 개발을 위한 기술 자문
- 지원기관: 라온시큐어 (6건) - FIDO 서버 설치 및 운영방법 그리고 안드로이드 환경에서의 FIDO 서비스 개발 노하우 지원
- 지원기관: 한국정보인증 (35건) - FIDO 서버를 응용서비스 제공(ASP) 형태로 개발하고 외부 결제서비스와 연동하기 위한 기술 자문 및 기술 지원

3) 비씨카드를 통하여 삼성 페이 서비스에 FIDO 인증서버를 적용 (‘15.8월~)

- 적용기술: FIDO 인증장치를 등록/인증/해지하는 기능을 제공하는 FIDO 서버 기술(ETRI), 모바일 카드 서비스(비씨카드)
- 서비스 제공방법: 비씨카드는 ETRI에서 기술이전 받은 FIDO 서버 기술을

이용하여 삼성페이에서 비씨카드로 결제를 할 경우 사용자 인증 서비스를 지문을 사용하여 FIDO 서버에서 처리

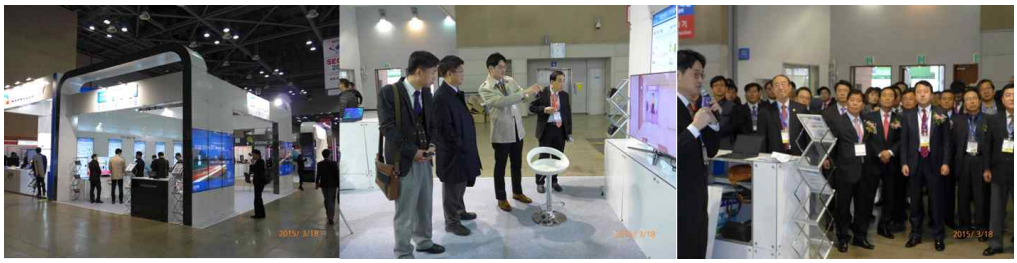
- 서비스 제공범위: 삼성전자의 갤럭시 S6와 노트 5에서 이용이 가능하고 현재 오프라인 비씨카드 전 가맹점에서 실제 신용카드 결제에 사용이 가능함

[그림 3-51] 비씨카드와 삼성페이를 이용한 간편결제 서비스

자. 전시회 참가

1) 세계 보안 엑스포 2015(SECON 2015)

- 2015.3.18.~3.20, KINTEX
- 국내외 총 396개 기관이 참가한 대규모 보안 전시회 참가
- ETRI 부스 방문객 1,500인 (행사 참관객 43,066명)
- 정부/유관기관/업체 등 관계자에게 오프라인 간편결제 등 기술 소개 및 시연



[그림 3-52] 보안엑스포 2015

2) 2015 IDB-IIC 연차총회 기술전시 참여

- 2015.3.26.~3.29, 부산 BEXCO
- K-ICT 부스에서 오프라인 간편결제 등 기술 소개 및 시연
- 2개 기술이전 기업(씽크풀, 쿠노소프트)과 공동 참여 – 상용 기술 홍보

[그림 3-53] 2015 IDB-IIC 연차총회

3) “ICT Spring Europe 2015” 기술전시 참여

- 2015.5.19.~5.20, 룩셈부르크 Kirchberg
- 주한룩셈부르크대표부의 참가 협조 요청을 받아, 핀테크 R&D 성과 전시 및 소개
- 2개 기술이전 기업(씽크풀, 쿠노소프트)과 공동 참여 – 상용 기술 홍보

[그림 3-54] ICT Spring Europe 2015

4) “2015 정보보호 R&D 및 제품전시회” 기술전시 참여

- 2015.7.8., 서울, 더케이호텔서울
- 핀테크 보안 기술 소개 및 시연

차. 보도 자료

1) 1) FIDO 국제 인증 획득

- FIDO 인증 제품
  - FIDO UAF 1.0 서버
  - FIDO UAF 클라이언트 (Android)
  - FIDO UAF Android 인증장치 (Password)
- 일시 : 2015년 5월 22일
- 방송 : YTN 사이언스
- 신문 : KBS, 중앙일보, 파이낸셜뉴스, 연합뉴스, 전자신문 외 다수

[그림3-55] ETRI, 세계 최초 FIDO 국제인증 방송 보도 - YTN 사이언스

2) FIDO 간편결제 시스템

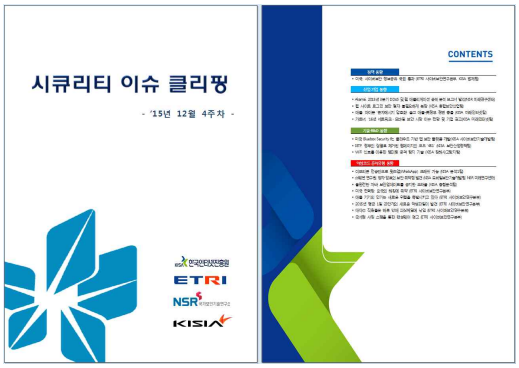
- '핀테크 산업' 협력 강화
  - BC카드, 삼성페이 인증기관 사업 참여 지원
  - BC카드, FIDO 기반 음성인증 모바일 결제 기술 지원
- 일시 : 2015년 7월 12일, 2016년 1월 14일
- 방송 : YTN 뉴스
- 신문 : 조선일보, 중앙일보, 서울신문, 경향신문, 전자신문 외 다수

[그림 3-56] BC카드, FIDO 기반 보이스 인증 결제 기술 개발 - 조선일보

카. 기술 동향 분석

1) 시큐리티 이슈 클리핑

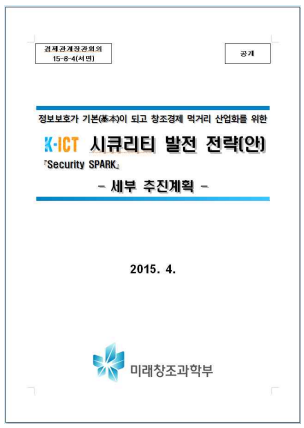
- 관계부처와 공동으로 해외의 관련기술 동향을 매주 수집 정리



[그림 3-57] 시큐리티 이슈 클리핑

2) K-ICT 시큐리티발전전략

- 이용자를 위한 편리한 보안(Usable Security) 기술 개발 보급 계획 수립
- 편리한 인증기술 확보, 무자각 프라이버시 보호, 차세대 전자인증 기술 개발, 핀테크 보안기술 확산
- 2015년 4월 미래창조과학부 장관회의에서 보고



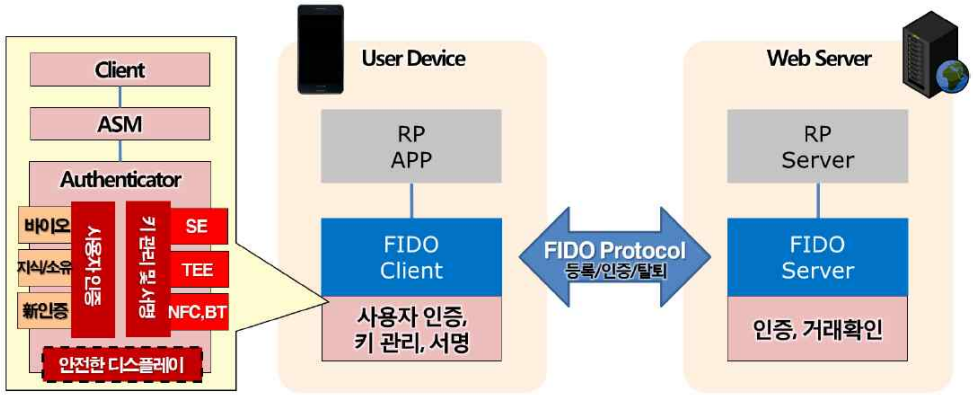
[그림 3-58] K-ICT 시큐리티발전전략

타. 시스템 개발

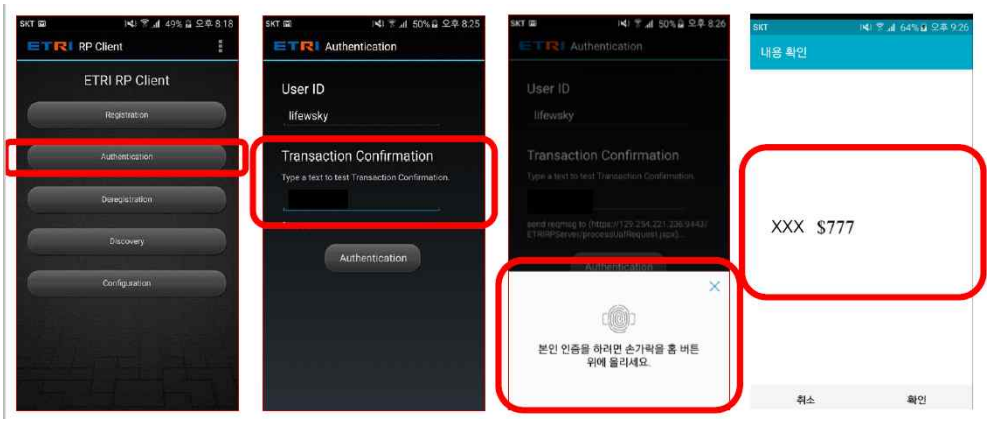
1) 개인정보 유통 보안 시스템 기술

○ FIDO 인증 기술

- 개발 내용
  - FIDO 서버
    . 사용자의 인증장치를 서버에 등록하고 등록한 인증장치를 이용하여 사용자를 인증하거나 전자서명으로 거래확인하는 기능을 제공하고 등록된 인증장치를 해지 하는 기능을 제공
    . 서버의 형상을 설정하고 인증장치를 관리하며 등록된 사용자와 인증정책 등을 설정하는 서버관리를 위한 Admin 화면제공
  - FIDO 클라이언트
    . FIDO 서버에 인증장치를 등록 또는 인증을 수행할 때 서버의 보안정책에 준용하는 인증장치 선별 및 선택하는 기능 제공
    . 다양한 인증장치와 모바일 앱을 연결하는 컴포넌트로 모바일 앱에서 FIDO 서비스를 호출하는 API를 제공
  - FIDO 인증장치
    . 사용자가 FIDO 서버에 등록 및 인증할 때 이용하는 PIN 기반의 소프트웨어 인증장치
    . 사용자 인증 및 전자서명을 포함한 암호처리 기능 제공



[그림 3-59] FIDO 인증 시스템 아키텍처



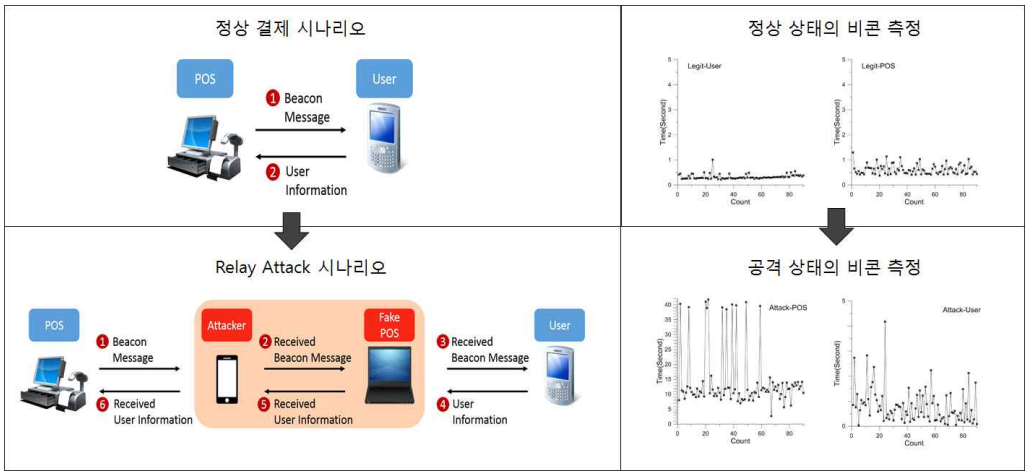
[그림 3-60] 지문인식 장치를 이용한 인증과 거래확인 서비스

2) 오프라인 피싱 방지

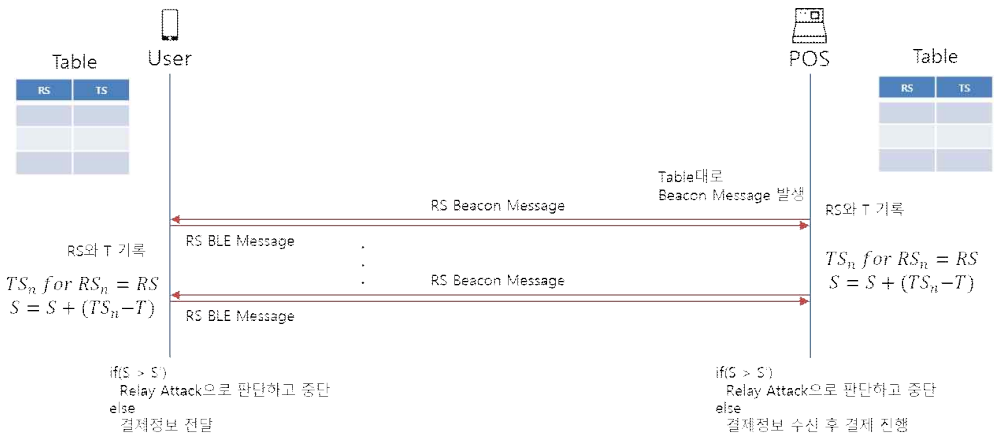
○ 악성 BLE 비콘 탐지 기술

- 개발 내용
  - BLE를 이용한 사용자의 결제/인증 서비스 시나리오에서 Relay Attack을 통해 공격자가 이득을 취하고 사용자가 피해를 볼 수 있는 부분에 대한 대응 수단으로서 악성 BLE 비콘 탐지 기술을 개발

- 개발된 보안 기술은 Relay Attack이 수행되는 경우 패킷 전송 지연이 발생한다는 점을 이용하여 RS(Random Sequence)를 이용한 보안 프로토콜을 설계하고 공격시나리오 구현을 통해 검증함



[그림 3-61] 악성 BLE 비콘 탐지 시나리오



[그림 3-62] RS를 이용한 악성 BLE 비콘 탐지 프로토콜

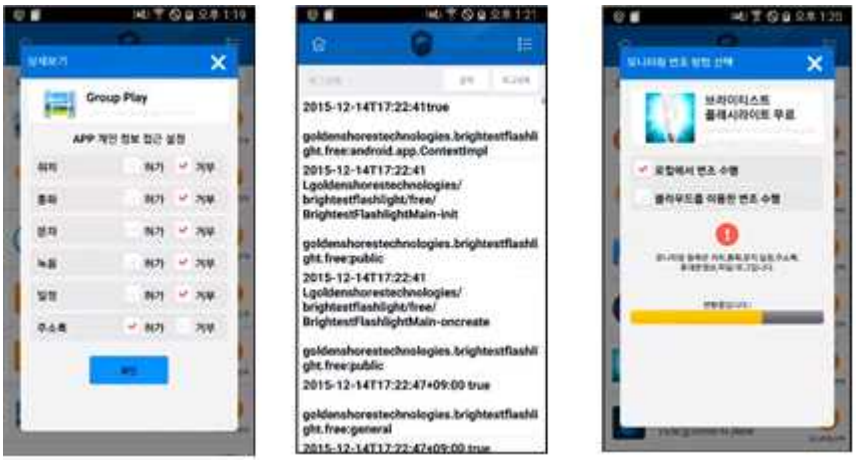
3) 개인정보 큐레이션 기술 개발

○ 개인정보 큐레이션 시스템

• 개발 내용

- 스마트폰 앱이 사용자의 개인정보를 접근하는 시점에, 사용자에게 해당 접근 내역을 알리고, 사용자의 승인 내역에 따라 개인정보를 제공하는 ‘실시간 개인정보 접근 제어 기능’ 개발
- 개인정보의 악용이 우려되는 스마트폰 앱을 대상으로 개인정보 접근 내역을 감시하는 ‘개인정보 접근 모니터링 설정 기능’ 개발
- 사용자가 스마트폰 앱에게 실시간으로 설정한 개인정보 정책을 조회하고 변경할 수 있는 ‘사용자 정책 관리 기능’ 개발
- 스마트폰 앱의 개인정보 접근 내역과 사용자의 개인정보 승인 내역을 조회할 수 있는 ‘로그 관리 기능’ 개발

[그림 3-63] 플래시 앱의 개인정보 접근 내역 알림 화면

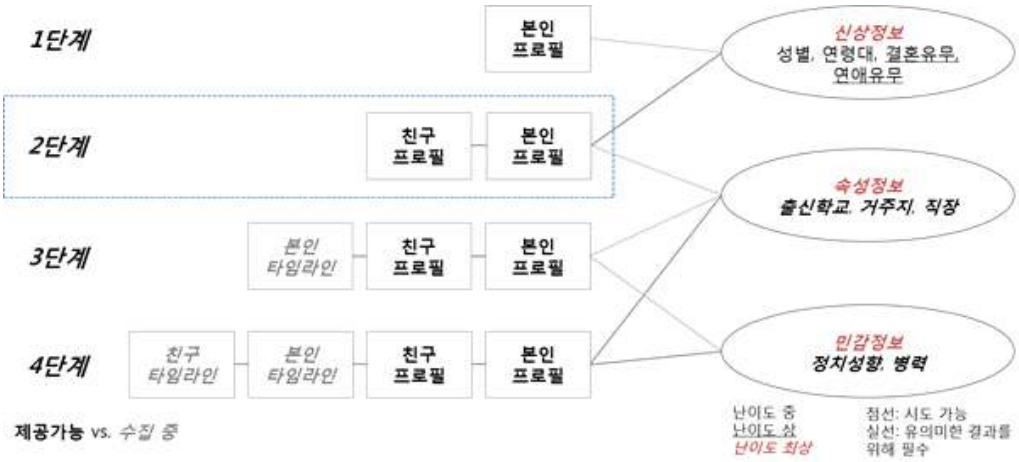


[그림 3-64] 개인정보 큐레이션 시스템의 기능별 UI

4) 개인정보 추론 리스크 분석 기술 개발

○ 개인정보 추론 리스크 분석 기술

- 개발 내용
  - 파일 및 SNS, 웹 상의 다양한 공개 정보들을 조합, 연결하여 유의미한 개인정보를 추론할 수 있는 다양한 방법론을 적용하여, 비정형 개인정보에 적합한 최적의 방법론을 찾고, 이 방법론을 적용하여 개인정보 추론 리스크를 분석
  - Facebook 사용자 데이터 기반
    - 성별: 90,966명 (남성 66,031명, 여성: 30,935명)
    - 연령: 515명
    - 기혼여부: 478명 (기혼: 365명, 미혼: 4,415명)
    - 연애여부: 4,780명 (연애 중(기혼 포함): 2,280명, 싱글: 2,552명)
  - 개인정보 추론 범위 설정



[그림 3-65] 개인정보 추론 범위 설정

- 사용자 성별 추론을 위해 파생 변수를 생성

변수명	형태	설명
military_yn	Binary	군 관련 직업 여부(1: 군관련 직업 종사(의무복무 포함), 0: 군 이외 직업 종사, <표 3> 참조)
job_male_yn	Binary	남성성이 강한 직업 종사 여부 (남성성이 강한 직업 리스트는 <표 4> 참조)
job_female_yn	Binary	여성성이 강한 직업 종사 여부 (여성성이 강한 직업 리스트는 <표 5> 참조)
female_school_yn	Binary	출신 고등학교/대학교명에 "여자" 단어의 포함 유무
male_highschool_yn	Binary	출신 고등학교명에 "공업" 단어의 포함 유무
interest_gender	Categorical	관심사항 (여성/남성/양성)
name_1st_male_ratio	Numeric	이름의 첫 번째 글자에 대한 남성성 정도 (<표 5 참조>)
name_2nd_male_ratio	Numeric	이름의 두 번째 글자에 대한 남성성 정도 (<표 5 참조>)

- 연령대 추론을 위해 파생 변수 생성

변수명	형태	설명
highschool_year	Numeric	고등학교 졸업 연도
university_year	Numeric	대학교 졸업 연도

- 기혼/연애 유무를 추론하기 위해 파생 변수를 생성

변수명	형태	설명
birthyear_lunar	Numeric	음력 생년
anniversary_yn	Binary	기념일 공개 유무
anniversary_year	Binary	기념일 연도 (기념일을 공개한 사용자의 경우)
gender	Binary	성별
military	Binary	군복무 여부
family_relation_yn	Binary	기혼자 가족관계 유무 (아들, 딸, 손자, 손녀, 시아버지, 시어머니, 장인, 장모)
highschool_year	Numeric	고등학교 졸업 연도
married_job	Numeric	기혼성향이 강한 직업 종사 여부 (점장, 이사, 팀장, 대표, 센터장, 이사, 부장, 수석, 소령, 중령, 대령, 상무, 전무, 아빠, 엄마, 주부, 차장, 사장, 시장, 소장, 교수, 실장, 최고경영자, 교장, 교감, 회장)

- 적용 알고리즘
  - 개인정보 추론시 크게 분류 기법(Classification)과 회귀분석 기법(Regression)으로 구분하여 적용
  - 실제 적용 알고리즘은 직관적인 결과 파악이 가능한 “Classification and Regression Tree” 알고리즘으로 결정

- 적용 결과
  - <성별> 추론 정확도 : 여성 - 66.8%, 남성 - 96.7%, 평균 - 80.4%
    * “군 관련 직업”의 영향으로 남성 예측 정확도가 높음
  - <나이> 추론 정확도 : 실제 나이대비 0.7년의 절대 오차. 실제 나이대비 오차율은 2.5%
  - <기혼 여부> 추론 정확도 :

Cut-Off 기준	정확도		
	기혼	싱글	평균
0.5	27.4%	99.0%	52.1%
0.924	70.7%	76.2%	73.4%

○ 비정형 개인정보 탐지 기술 고도화

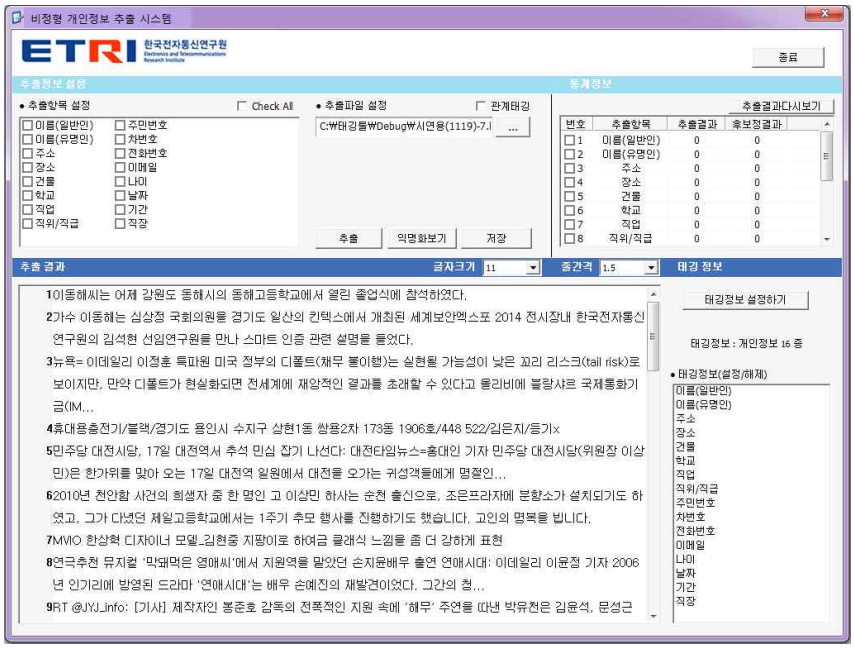
- 개발 내용
  - 개인정보 추론을 위한 공개 정보내에서 비정형 개인정보를 찾을 수 있도록 기존 탐지대상을 확대하여 개인정보 탐지 기술을 고도화
  - Facebook 사용자 프로파일 데이터 수집
  - Facebook 사용자 프로파일 데이터중 이름, 직업, 기타 개인정보 추론 가능 단어의 정보 분석

Attributes	Type	N. collected	Ratio	Attributes	Type	N. collected	Ratio
User_ID	Num	111,123	100%	Birth_Year	Num	4,247	3.82%
Name	Char	111,123	100%	Birth_Year_Lunar	Num	6,105	5.49%
Gender	Char	96,966	87.26%	Blood_Type	Char	60,828	54.74%
Location_State	Char	66,539	59.88%	Interest (M/F/Both)	Char	24,279	21.85%
Location_City	Char	34,957	31.46%	Wesite	Char	3,753	3.38%
Birthplace_State	Char	65,604	59.04%	Language	Char	21,005	18.90%
Birthplace_City	Char	37,398	33.65%	Relationship_Status	Char	4,780	4.30%
Graduate_School	Char	1,941	1.75%	Wedding_Day	Date	178	0.16%
Graduate_School_Location_State	Char	1,454	1.31%	Anniversary	Date	1,189	1.07%
Graduate_School_Year	Num	10	0.01%	Political_Opinion	Char	735	0.66%
University	Char	54,666	49.19%	Technology	Char	1,455	1.31%
University_Location_A	Char	49,290	44.36%	Spouse	Char	106	0.10%
University_Year	Num	2,322	2.09%	Nickname	Char	49	0.04%
Highschool	Char	57,728	51.95%	Lived_Place_List	List	1,838	1.65%
Highschool_Location_A	Char	52,138	46.92%	Work_List	List	48,653	43.78%
Highschool_Year	Num	5,952	5.36%	Family_List	List	21,905	19.71%

[그림 3-66] 사용자 프로필상 속성 데이터 및 수집율

  - 전년도 개발 형태소 분석기 업그레이드
  - 비정형 개인정보 탐지 프로그램 개발 – TXT, HWP 파일을 열어 개인정보 추출후 변환 저장

- 개발 결과
  - 비정형 개인정보 추출 시스템



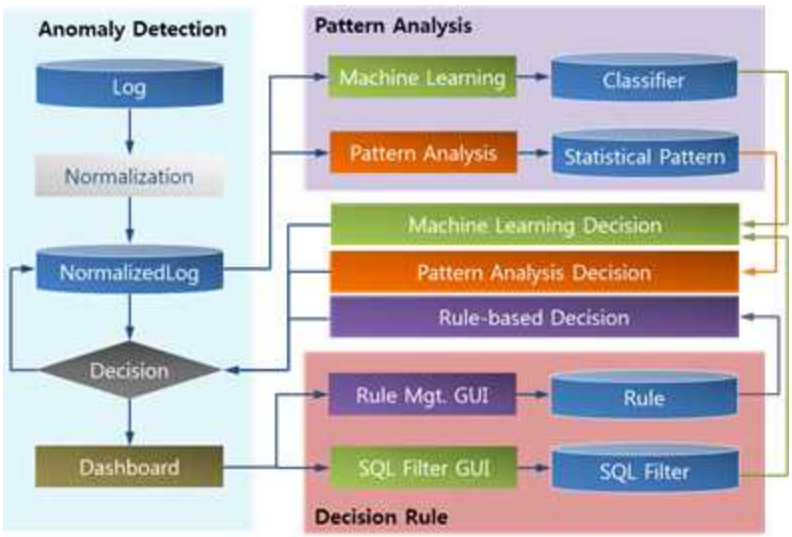
[그림 3-67] 비정형 개인정보 추출 시스템 화면

[그림 3-68] 비정형 개인정보 추출 결과

5) 개인정보 이상접근 탐지 기술 개발

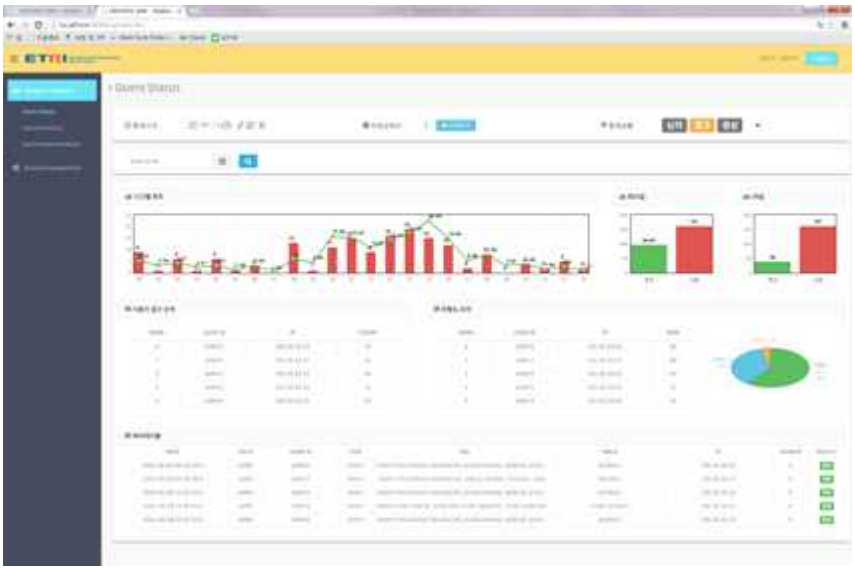
○ 개인정보 이상 접근 탐지 기술

- 개발 내용
  - 기계학습, 사용자 패턴, 관리자 규칙 등을 이용하여 데이터베이스에 접근하는 이상행위를 탐지하여 개인정보를 보호하는 기술



[그림 3-69] 이상행위 탐지 시스템 구조도

  - 발생하는 SQL 구문을 분석하여 자주 사용하는 명령어, 접근하는 테이블 및 필드 등으로부터 사용자의 특성을 추출하고, 기계학습 기법을 이용하여 이상 접근을 탐지
  - 사용자의 데이터베이스 접근 횟수, IP 주소, 접근 시간 등을 기반한 사용자 패턴 분석
  - 관리자 규칙을 이용한 이상행위 접근 제어



[그림 3-70] 이상행위 탐지 모니터링 시스템

- 데이터베이스 이상행위 탐지 모니터링 시스템
  . 쿼리 발생을 시간별, 요일별, 일별로 분석하여 데이터베이스 접근 현황을 실시간으로 분석
  . 특정 사용자의 접근 패턴, 특정 테이블에 대한 접근 패턴을 분석
  . 관리자 규칙 설정, 이상행위 판단을 위한 가중치 설정

제 4 절 시장 현황 및 사업화 전망

1. 시장 현황

가. 개인정보 유통 관련 시장 현황

○ 통계청 자료에 따르면 국내 모바일 간편 결제 시장은 2013년 1분기 1조 1천 270억원 규모에서 2014년 1분기 2조 8천 220억원, 2015년 1분기 5조 936억 원으로 매년 두 배씩 성장하고 있음

○ 국외에서는 애플페이를 시작으로 삼성페이, 구글페이 등이 시장을 선점하기 위해 치열하게 경쟁하고 있고 국내에서도 삼성페이를 필두로 카카오페이, 네이버 페이 등이 서비스를 시작하여 이 시장에서 주도권을 잡기위해 치열하게 경쟁하고 있음

나. 안티 피싱/파밍 시장 현황

○ 메모리 해킹 공격을 막기 위한 다양한 솔루션이 개발되었음. 큐브피아 '권가 금융해킹방지솔루션', 이니텍 '이니세이프샌드박스', 시큐브 '스마트 그리핀', 카스퍼스키랩 '카스퍼스키 프러드 프리밴션', 소프트포럼 '제큐어투웨이', 마크애니 '이뱅킹세이퍼', 잉카인터넷 '엔프로텍트 X가드' 등의 솔루션이 존재함

○ FIDO 얼라이언스의 범용인증 표준, 거래 연동 OTP, 추가 인증 시스템, 이상 징후 탐지 시스템, 입금계좌 지정제 개선 등 금융 서비스의 메모리 해킹을 포함한 신종 피싱 공격에 대응하는 인증 강화 솔루션이 활발하게 적용됨

○ 국내의 피싱차단건수는 2010년 8건에서 2015년 7월 4,842건으로 5년간 600배 이상 증가했음. 또한 파밍 차단 건수는 2012년 110건에서 2015년 7월 5956건으로 3년간 50배 증가했음. 또한 파밍 피해액은 2015년도 상반기만 200억원을 넘어섬[7)]

다. 빅데이터 개인정보 보호 관련 현황

○ 빅데이터 환경을 이용하는 다양한 정책이 개발되고 있음

- 2012년 11월, '스마트 국가 구현을 위한 빅데이터 마스터플랜' 발표
- 2013년 5월, '정부3.0 기본계획'에서는 개인정보보호 대책 제시
- 2013년 9월, 안전행정부 '공공정보 개방 공유에 따른 개인정보보호 기술 가이드라인' 발표
- 2013년말, 방송통신위원회 '빅데이터 개인정보 보호 가이드라인' 초안 발표
- 2014년 8월, 온라인상 수집한 주민번호 파기 기한 종료
- 2014년 11월, 방통위, 온라인 개인정보 취급 가이드라인 발표
- 2016년 1월, 미래부 및 방통위, 빅데이터/사물인터넷/클라우드 서비스 활성화를 위한 비식별 정보의 선활용 후거부 등 개인정보 규제를 풀어 '빅데이터' 시장 활성화에 추진 계획 발표

○ 전세계 빅데이터 시장 규모 해당부분은 한국전자통신연구원에서 저작권을 확보하지 못하여 공개대상에서 제외되었습니다

○ 개인정보 노출을 원천적으로 차단하는 기술은 아직 이론 단계에 머물러 있으며, 실제 필드에서는 단순한 정형 개인정보에 대한 암호화/비식별화 기술만 적용됨

○ 온라인/빅데이터 개인정보 탐지는 주민번호와 같은 정형 식별정보 수준에 머물러 있으며, 개인정보 삭제 서비스도 비용상의 문제와 효과에 한계가 있음

---

7) 데일리한국, 국내 파밍 사기, 올해 들어 6000건, 피해액 상반기만 200억, 2015.8

2. 국내외 여건 변화 및 대응 전략

○ 아래 표는 지난 1년 동안 국내 및 국외의 표준화, 기술적, 사회적 및 정책적 여건 변화와 이에 대한 본 과제의 대응전략을 나타내고 있음

[표 3-7] 국내외 여건 변화 및 대응 전략

세부 분야	국내외 여건 변화	대 응 전 략
정책적 여건	○ 공인인증서 관련하여 비표준 기술인 액티브X의 사용에 대하여 이용상의 불편함과 보안상의 취약점이 발생하여 대체 인증기술의 개발이 시급한 상황이며, 핀테크의 등장으로 보안적으로 강력하면서 사용하기 간편한 인증기술의 필요성이 부각됨	○ 글로벌 표준기반의 FIDO 인증 기술 개발 - 보안토큰 또는 바이오 정보를 이용한 인증장치를 이용하는 FIDO 간편인증 기술을 개발함 - 개발 기술의 국제경쟁력을 가추기 위해 FIDO 상호운영성 시험을 수행함
	○ 한국은행과 금융결제원은 “금융분야 바이오인증 활성화 전략 세미나”를 개최하고 국내 바이오인증 표준 기술 규격안을 개발하기로 결정함	○ 바이오정보 기반의 인증기술 확산을 위해 FIDO 간편인증 기술을 개발하고 업체 기술이전하여 지문/화자/얼굴 인식 등의 기술에 접목하여 서비스를 개발 중에 있음
	○ “미래부와 인터넷진흥원은 ‘해킹, 전자금융사기 예방체계’를 구축하였지만 늘어나는 파밍 시도에는 대처에 어려움	○ 피싱/파밍 공격 현황을 조사하여 기존 전자금융사기 방안들의 특징을 분석하고, 새로운 타입의 공격 및 대응 방안을 제시하여 조기 대응 강조
	○ 미래부와 방통위는 빅데이터 시장	○ 비정형 개인정보 추출 및 비식별

세부 분야	국내외 여건 변화	대 응 전 략
	활성화를 위해 비식별 정보의 선 활용이 가능하도록 규제 개혁을 추진중	화 기술 개발로 빅데이터 시장 활성화에 기여할 수 있도록 대응
기술적 여건	○ 스마트폰에 지문인식 장치가 탑재되어 사용자의 바이오 정보를 이용하여 인증이 가능함 ○ 정상적인 스마트폰 앱으로 위장하고 사용자의 개인정보를 임의로 탈취하는 공격이 활발하게 이루어짐 ○ 빅데이터 처리 기술의 발달로 공공 분야를 비롯한 정보 공유가 시작되고 있음	○ FIDO 서버 및 클라이언트 기술을 개발하여 스마트폰의 지문인식장치를 인증장치로 사용하여 사용자를 인증하는 기술 개발 ○ 스마트폰 앱의 개인정보 접근을 모니터링하여 실시간으로 대응할 수 있는 개인정보 큐레이션 기술 개발 추진 ○ 빅데이터 공유에 선행되어야할 프라이버시 필터링 기술 개발 강화
표준화 여건	○ 패스워드 없이 사용자를 간편하게 인증하는 글로벌 표준인 FIDO가 등장하여 널리 보급됨	○ FIDO에 Sponsor 회원으로 가입하여 표준기술 동향을 파악하고 기술을 개발하여 상호운영성 시험에 참가하여 기술의 국제경쟁력을 제공함
사회적 여건	○ 지문인식 외에도 사용자의 음성 및 얼굴 등을 이용하여 사용자를 간편하게 인증하길 원하나 실제 적용하는데 어려움이 있음	○ FIDO 기술이전을 통하여 모바일 결제 환경에서 화자 또는 얼굴 인증하는 기술과 접목하는 부분을 기술지원을 통하여 해결함

세부 분야	국내외 여건 변화	대 응 전 략
	○ 인터넷 피싱/파밍에 대한 기술이 고도화됨에 따라 사용자들의 불편함과 우려 확대 ○ 빅데이터 활용 서비스의 증가가 예상됨	○ 사용자가 쉽고 안전하게 사용할 수 있는 UX와 보안기능에 초점을 맞춘 안티 피싱/파밍 기술을 개발 ○ 빅데이터 프라이버시 보호 기술에 대한 홍보를 강화하여 빅데이터 시대에 안전한 활용 가능성을 높임

3. 사업화 전망

- FIDO 기술은 이미 삼성페이에 적용되어 상용서비스를 제공하고 있어 다양한 업체에서 기술이전을 받고 2016년에는 본격적으로 사업화가 가능할 것으로 전망됨
- 향후 결제 및 금융서비스에서 FIDO 기술이 적극 활용될 것으로 예상되며 FIDO가 널리 보급될수록 바이오 인식 기술과의 연계를 통하여 다양한 사업화 기회가 창출될 것으로 예상됨
- 피싱/파밍 공격은 다른 공격 기술 및 사회공학적인 방식과 접목하여 보다 지능적이고 고도화되는 추세이므로, 가능한 피싱 공격 방법을 찾아내고 대응 방법을 선행적으로 연구하는 분야와 사용자의 편의성을 개선하는 기술 개발을 통해 수요가 꾸준히 증가할 것으로 예상
- 개인정보 스캐닝/필터링 관련 업계에서는 비정형 비식별 개인정보 노출 탐지를 차세대 개인정보보호 핵심 기술로 인식하고 있으나, 비정형 정보처리 및 추론 기술 등 관련 기술 기반이 부족하여 이를 직접 개발하지 못하고 있는 상황으로 본 기술을 활용한 다양한 사업화 기회가 창출될 것으로 예상

제 5 절 기업 재무건정성 현황

○ 과제명 : 시큐리티 큐레이션을 제공하는 프라이버시강화형 개인정보 유통보안 핵심기술 개발

○ 주관기관: 한국전자통신연구원

* 비영리 법인으로 기업 재무건전성 현황 작성 면제 대상임

○ 과제명 : 개인정보기반 스마트결제·공유 인터랙션 기술 개발

○ 참여기관: ㈜비씨카드

[표 3-8] 재무건전성 현황

<table>
<tr><th>항 목</th><th colspan="3">해당사항기재</th></tr>
<tr><td>최근년도말 부채비율
(산식 : 부채총계/자기자본총계×100)</td><td colspan="3">○ 계산결과 : 201.7%
○ 부채총계 19,325억 / 자기자본총계 9,581억</td></tr>
<tr><td>최근년도말 유동비율
(산식 : 유동자산/유동부채×100)</td><td colspan="3">○ 계산결과 : 130.1%
○ 유동자산 22,643억 / 유동부채 17,400억</td></tr>
<tr><td>이자보상비율
(산식 : 영업이익/이자비용)</td><td colspan="3">○ 계산결과 : -
○ 영업이익 2,694억 이자비용 0</td></tr>
<tr><td rowspan="3">3개년도 계속 적자 기업(kisline활용)
(판단기준 : 손익계산서 상의 당기순이익(손실)로서 판단)</td><td colspan="3">○ 해당사항없음</td></tr>
<tr><td>20 년</td><td>20 년</td><td>20 년</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td>자본잠식여부 (법정관리, 화의기업여부 등)</td><td colspan="3">○해당사항없음</td></tr>
<tr><td>외부감사 기업의 경우 최근년도 감사의견이 “한정”인 경우</td><td colspan="3">○해당사항없음</td></tr>
<tr><td>중소기업 해당여부</td><td colspan="3">○해당사항없음</td></tr>
<tr><td>-상시근로자수가 1천명 이상인 기업</td><td colspan="3">○해당사항없음</td></tr>
<tr><td>-자산총액이 5천억원 이상인 법인 또는 그러한 법인이 기업 발행주식 총수의 30%이상을 소유하고 있는 기업</td><td colspan="3">○해당사항없음</td></tr>
<tr><td>-상호출자제한기업집단에 속하는 회사</td><td colspan="3">○해당사항없음</td></tr>
<tr><td>기타 특이사항</td><td colspan="3">○해당사항없음</td></tr>
</table>

제 4 장 연구개발결과의 활용 계획

제 4 장 연구개발결과의 활용 계획

1. 연구개발결과의 활용 계획

○ FIDO 인증 기술

- 사용자의 다양한 생체정보를 이용하여 전자결제 서비스의 사용자 간편 인증 솔루션으로 활용이 전망됨
- 핀테크 사업에서 사용자의 본인인증 및 전자서명을 이용하여 거래확인 서비스에 활용이 가능함
- 현재 공인인증서로 사용하고 있는 사용자 확인 및 전자서명 서비스에 대해 대체인증 기술로 사용될 수도 있음

○ 악성 BLE 비콘 탐지 기술

- 지불/결제 관련 업체의 BLE 비콘 기반 오프라인 간편 결제 솔루션에 대한 보안취약성을 개선할 수 있는 방법으로 활용
- 출입통제 관련 업체의 BLE 비콘 기반 오프라인 간편 인증 솔루션에 대한 보안취약성을 개선할 수 있는 방법으로 활용
- 지불/결제, 출입통제 솔루션 이외에도 다양한 무선 신호 기반의 간편 인증 기술에 적용하여 보안성이 강화된 새로운 솔루션 개발에 활용

○ 개인정보 큐레이션 시스템

- 악성코드가 숨겨진 앱의 프라이버시 침해를 실시간으로 차단하는 서비스에 활용
- 사용자의 어플리케이션 사용 패턴을 인지하고, 특정 상황에서 이상패턴을 감지하여 추가 인증을 요청하는 보안 서비스 연구 개발에 활용
- MAM(Mobile Application Management) 관련 제품에서 바이너리 앱의

보안성 강화를 위한 보안 모듈 주입(App wrapping) 기능 개발에 활용

○ 개인정보 추론 리스크 분석 기술

- 개인정보 추론을 통해 민감정보가 아닌 일반 정보들을 기존 개인정보와 연계하여 개인의 민감정보를 도출할 수 있음을 확인한 것으로, 개인정보에 한정하지 않고 다양한 영역에서 추론 기법을 확대 적용이 가능함
- 개발된 기술을 비정형 개인정보 탐지 기술과 연계하여, 빅데이터 환경에서 개인정보보호 고도화에 적용시, 빅데이터 공개전 개인정보 삭제 대상의 확대가 가능하고, 빅데이터 활용 시 보다 개인정보 노출 가능성을 감소시킬 것으로 예상됨

○ 개인정보 이상 접근 탐지 기술

- 개인정보 유출 사고의 90% 이상이 데이터베이스에서 발생하고 있어 데이터베이스 보안이 시급한 상황이나, 지금까지의 기술은 데이터베이스 암호화, 데이터베이스 접근 제어에 국한되어 있음
- 적법한 사용자가 데이터베이스에 접근하여 개인정보를 탈취하는 공격을 방어하기 위해서는 기존의 접근 방식과 다른 행위임을 파악하여 차단하는 방법이 우선적임
- 이상 접근 탐지 기술은 기계학습, 사용자 패턴 등을 이용하여 데이터베이스에 접근하는 행위를 분석하는 기술로 데이터베이스 접근 및 FDS 기술에 활용될 수 있음

제 5 장 결 론

제 5 장 결 론

본 과제는 스마트 환경의 다양한 개체들로부터 안전하고 편리한 스마트 서비스를 제공받기 위하여 리스크/협상에 기반한 시큐리티 큐레이션을 제공하는 프라이버시 강화형 개인정보 유통 보안 핵심 기술을 개발을 목표로 2013년부터 2015년까지 수행되었다. 본 사업은 비씨카드와 공동연구를 함으로써 정보보호 시장과 금융권 시장의 요구사항을 현실적으로 반영한 기술을 개발하였다.

본 과제에서 수행된 FIDO 인증 기술은 FIDO 상호운영성 시험을 수행하여 국제 인증을 획득하였으며, ETRI에서 기술이전을 받은 비씨카드는 FIDO 서버 기술을 삼성페이에 적용하여 현재 오프라인 비씨카드 전 가맹점에서 실제 신용카드 결제가 가능하다. 또한 FIDO 인증 기술은 15개 업체에 기술이전 되어 다양한 분야에 활용될 예정이다.

핸즈프리 결제 시스템은 비컨을 이용한 간편한 결제 기술로 FIDO 기술이 적용되어 있으며 비씨카드의 온오프라인 통합 간편결제 ZEP 서비스에 활용되었다.

스마트폰 환경에서 개인의 정보를 보호하기 위하여 스마트폰 앱들이 접근하는 사용자의 개인정보 내역을 감시하고 제어하는 개인정보 큐레이션 기술을 개발하였고, SNS, Facebook, 웹 상의 다양한 공개 정보를 이용하여 개인정보를 추론하는 것을 방지할 수 있는 개인정보 추론 리스크 분석 기술을 개발하였다.

또한, 데이터베이스에 접근하여 개인정보를 탈취하는 사건을 방지하기 위하여 기계학습, 사용자 패턴, 관리자 규칙 등을 이용한 데이터베이스 접근 이상행위 탐지 기술을 개발하였다.

이러한 연구 결과는 논문 및 특허, 표준화 활동 등의 연구실을 도출하였으며, 기술이전을 통하여 실용화되고 있다.

제 6 장 연구시설·장비 현황

제 6 장 연구시설·장비 현황

구입 기관	연구시설/ 연구장비명	규격 (모델명)	수량	구입 연월일	구입 가격 (천원)	구입처 (전화번호)	비고 (설치 장소)
ETRI	오프라인 개인정보 공유 인터랙션 프로토타입 시스템 구현	시작품	1	2013.7	65,780	㈜듀얼아이 (031-213-0074)	ETRI
ETRI	아이덴티티 데이터마이닝 검색 시스템 시제품 개발	시작품	1	2013.8	65,330	㈜유엠로직스 (042-365-0095)	ETRI
ETRI	스마트채널3 구현	시작품	1	2013.8	66,030	㈜케이사인 (02-564-0182)	ETRI
ETRI	웨어러블장치 기반의 인증서비스 프로토타입 구현	시작품	1	2013.9	41,220	㈜쿠노소프트 (070-7503-4855)	ETRI
ETRI	DB 비정상 행위 탐지 모델 및 서버 사용자 인터페이스 구현	시작품	1	2014.6	93,830	㈜케이사인 (02-564-0182)	ETRI
ETRI	In-Store 개인정보 유통 보안 인터랙션 프로토타입 시스템 구현	시작품	1	2014.7	63,360	㈜듀얼아이 (031-213-0074)	ETRI
ETRI	스마트 단말용 보안 기능 검증 응용 서비스 구축	시작품	1	2014.9	65,830	㈜익스트러스 (02-6928-6774)	ETRI

구입 기관	연구시설/ 연구장비명	규격 (모델명)	수량	구입 연월일	구입 가격 (천원)	구입처 (전화번호)	비고 (설치 장소)
ETRI	안드로이드 시스템 레벨 취약점 및 해킹 분석 도구 개발	시작품	1	2014.9	41,320	㈜라닉스	ETRI
ETRI	유통 보안 인터랙션 응용서비스 프로토타입 개발	시작품	1	2015.6	68,530	㈜듀얼아이	ETRI
ETRI	이용자 단말 지키미 앱 구현	시작품	1	2015.8	55,330	(주)유엠로직스	ETRI
비씨카드	POS 결제 플랫폼 인터페이스 표준 결제 UI/UX 개발	시작품	1	2013.12	25,500	아스텝즈 주식회사	비씨카드
비씨카드	ZEP 서비스 (Hands-Free Payment) 서비스 단말개발	시작품	1	2014.12	49,940	(주)아스텝즈	비씨카드
비씨카드	ZEP 서비스 (Hands-Free Payment) 서비스 WAS 개발	시작품	1	2014.12	29,850	(주)이포넷	비씨카드
비씨카드	화자인증 서비스 구축	시작품	1	2015.12	69,960	파워보이스	비씨카드

부 록

1. 특허

순번	특허명	출원번호	출원국	출원일	발생차수
1	클라우드 ID 카드를 이용하여 개인 정보를 제공하기 위한 시스템 및 그 방법	10-2013-0055877	한국	2013.05.16	1차년
2	모바일 기기의 유해 정보를 검증하기 위한 시스템 및 그 방법	10-2013-0057985	한국	2013.05.22	1차년
3	웹 사이트 검증 장치 및 그 방법	10-2013-0059102	한국	2013.05.24	1차년
4	사용자단말을 통해 IC카드를 관리하고 이용하는 방법 및 장치	10-2013-0076554	한국	2013.07.01	1차년
5	개인정보 소유자 식별 장치 및 방법	10-2013-0106500	한국	2013.09.15	1차년
6	코퍼스 자동 구축 방법 및 이를 이용한 개체명 인식 방법과 장치	10-2013-0131596	한국	2013.10.31	1차년
7	보안 도우미 서비스 제공장치 및 서비스 제공방법	10-2013-0137901	한국	2013.11.13	1차년
8	휴대 단말기, 단말기 및 보안쿠키를 이용한 인증 방법	10-2013-0142828	한국	2013.11.22	1차년
9	모바일 인증 시스템 및 방법	10-2014-0003451	한국	2014.01.10	2차년
10	문자 인식의 후처리 방법 및 이를 이용하는 문자 인식 장치	10-2014-0008485	한국	2014.01.23	2차년
11	전자 서명 제공 장치 및 방법	10-2014-0014991	한국	2014.02.10	2차년
12	IC 카드를 인증 매체로 이용하기 위한 방법, 장치 및 시스템	10-2014-0065285	한국	2014.05.29	2차년
13	구역 기반의 사용자확인 시스템과 그 방법 및 구역 기반의 사용자확인 서버	10-2014-0117686	한국	2014.09.04	2차년
14	Device and method for providing security assistant service	14/243,081	미국	2014.04.02	2차년
15	System and method for security authentication via mobile device	14/337,881	미국	2014.07.22	2차년
16	Mobileterminal, terminal and authentication method using security cookie	14/516,141	미국	2014.10.16	2차년

순번	특허명	출원번호	출원국	출원일	발생차수
17	Apparatus and method for providing digital signature	14/617,187	미국	2015.02.09	3차년
18	Zone-based user verification server, system, and method therof	14/699,328	미국	2015.04.29	3차년
19	유사 사용자 식별 장치, 시스템 및 그 방법	10-2015-0065283	한국	2015.05.11	3차년
20	비정형 데이터 추출 및 익명화 장치	10-2015-0073063	한국	2015.05.26	3차년
21	프라이버시 보호 시스템 및 방법	10-2015-0082868	한국	2015.06.11	3차년
22			한국		3차년
23			미국		3차년

2. 논문

순번	구분	논문 제목	학술지 명칭	주저자	게재 연월	SCI 구분	발생 차수
1	국내 게재	모바일 전자 영수증	TTA 저널	김수형	2013.04	N	1차년
2	국내 게재	액티브 피싱 공격 및 대응방안 고찰	ETRI 정보통신동향분석	김승현	2013.05	N	1차년
3	국내 게재	금융기관을 타켓으로하는 피싱파밍 공격 기술 동향	대한전자공학회지	김승현	2013.08	N	1차년
4	국제 발표	Geo-Location based QR-Code Authentication Scheme to Defeat Active Real-Time Phishing Attack	ACM CCS DIM 2013	김승현	2013.11	N	1차년
5	국내 발표	비정형 사용자 이름을 정형화된 한글 이름으로 변환하는 방법 연구	한국정보과학회 추계학술발표대회	김석현	2013.11	N	1차년
6	국내 게재	SNS에 노출된 개인정보의 소유자 식별 방법	한국정보보호학회 논문지	김석현	2013.12	N	1차년
7	국내 게재	빅데이터 개인정보 위험 분석 기술	한국정보보호학회지	최대선	2013.06	N	1차년
8	국내 게재	소셜네트워크서비스 개인정보 노출 실태 분석	한국정보보호학회 논문지	최대선	2013.10	N	1차년
9	국내 발표	공공정보 개방 공유에 따른 개인정보보호 기술검토	한국정보과학회 추계학술발표대회	최대선	2013.11	N	1차년
10	국내 발표	자동 구축된 코퍼스를 이용한 비정형 개인정보 탐지 기법	한국정보과학회 추계학술발표대회	조진만	2013.11	N	1차년

순번	구분	논문 제목	학술지 명칭	주저자	게재 연월	SCI 구분	발생 차수
11	국내 발표	페이스북과 트위터 이용자 계정 연결 방법	한국정보과학회 추계학술발표대회	박준범	2013.11	N	1차년
12	국내 발표	터치사인 온라인 시스템 구현	대한전자공학회 하계학술대회	김수형	2014.06	N	2차년
13	국내 발표	아이핀(i-PIN) 서비스에 대한 액티브피싱 공격	대한전자공학회 하계학술대회	김승현	2014.06	N	2차년
14	국내 발표	터치사인 오프라인 전자서명 시스템 구현	대한전자공학회 하계학술대회	조영섭	2014.06	N	2차년
15	국내 발표	목표 문자열을 이용한 문자 인식 판별 방법	한국통신학회 하계종합학술발표	노종혁	2014.06	N	2차년
16	국제 발표	Device Control Protocol using Mobile Phone	ICACT 2014	노종혁	2014.02	N	2차년
17	국내 발표	관계형 데이터베이스에서 준식별자를 이용한 익명화 처리 기법	한국정보보호학회 추계학술대회	박준범	2014.06	N	2차년
18	국내 발표	iBeacon 기술 동향 및 문제점 분석	한국정보과학회 한국컴퓨터종합학술대회	김대엽	2014.06	N	2차년
19	국내 발표	다중 소셜 네트워크 서비스 간에 사용자 연결 방법	한국정보처리학회 추계학술대회	김석현	2014.11	N	2차년
20	국내 발표	온라인 중고물품판매에 대한 개인정보노출 위험	한국정보처리학회 추계학술대회	박준범	2014.11	N	2차년
21	국내 발표	터치사인 인증서 관리 시스템 구현	대한전자공학회 하계학술대회	조상래	2014.06	N	2차년
22	국내 게재	패스워드 없는 인증기술:FIDO	ETRI 전자통신동향분석	조상래	2014.11	N	2차년
23	국내 발표	FIDO UAF 1.0 서버 구현	한국정보처리학회 추계학술대회	김석현	2015.10	N	3차년

순번	구분	논문 제목	학술지 명칭	주저자	게재 연월	SCI 구분	발생 차수
24	국내 발표	일반화와 데이터삽입을 이용한 익명화 처리 기법	한국정보처리학회 추계학술대회	박준범	2015.04	N	3차년
25	국제 발표	The privacy analysis of online trade market	Internation Conference on Social Science and Psychology	박준범	2015.06	N	3차년
26	국제 발표	Effects of Contextual Properties on Users' Privacy Preferences in Mobile Computing Environments	The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications	김승현	2015.08	N	3차년
27	국제 발표	Accurate Indoor Proximity Zone Detection Based on Time Window and Frequency with Bluetooth Low Energy	The 12th International conference on Mobile Systems and Pervasive Computing	김대엽	2015.08	N	3차년
28	국내 게재	핀테크 기술 및 보안 동향	전자통신동향분석	이성훈	2015.08	N	3차년
29	국내 게재	자바스크립트 변조를 이용한 국내 인터넷 뱅킹 키보드 암호화 모듈 우회 공격	한국정보보호학회 논문지	이성훈	2015.08	N	3차년
30	국내 게재	관계형 데이터베이스에서 데이터 그룹화를 이용한 익명화 처리 기법	한국정보보호학회 논문지	박준범	2015.06	N	3차년
31	국제 게재	Estimating Korean Residence Registration Numbers from Public Information on SNS	IEICE Transaction on Communications	최대선	2015.04	Y	3차년

순번	구분	논문 제목	학술지 명칭	주저자	게재 연월	SCI 구분	발생 차수
32	국제 게재	Short Dynamic Group Signature Scheme Supporting Controllable Linkability	IEEE Transaction on Information Forensics and Security	황정연	2015.06	Y	3차년
33	국제 게재	Customer Data Scanner for Hands-Free Mobile Payment	IEICE Transaction on Communications	김수형	2015.11	Y	3차년
34	국제 게재	New Efficient Batch Verification for an Identity-Based Signature Scheme	Security and Communication Networks	황정연	2015.01	Y	3차년

3. 표준화

가. 국내 표준화 성과

순번	표준명	발행 기관 (국)	채택 여부	제안자	채택번호	발생 차년
1	POS 단말기 사용자 인터페이스	TTA (한국)	채택	장석호	TTAK.KO-12.0250	1차년
2	POS 단말기 결제 모듈 인터페이스	TTA (한국)	채택	장석호	TTAK.KO-12.0227	1차년
3	NFC P2P기반 모바일 전자 영수증 관리 규격	TTA (한국)	채택	김수형	TTAK.KO-12.0224	1차년
4	모바일 단말을 이용한 디바이스 제어 프로토콜 및 보안 기능 (표준특허)	TTA (한국)	채택	노종혁	TTAK.KO-12.0225	1차년
5	자바 스크립트 객체 표기법 (JSON) 웹 전자서명	TTA (한국)	채택	조상래	TTAI.IF-12.0003	1차년
6	자바 스크립트 객체 표기법 (JSON) 웹 키	TTA (한국)	채택	조상래	TTAI.IF-12.0002	1차년
7	자바 스크립트 객체 표기법 (JSON) 객체 서명 및 암호화를 위한 요구사항	TTA (한국)	채택	조상래	TTAI.IF-12.0001	1차년
8	대면거래에서의 전자서명 규격	TTA (한국)	채택	김수형	TTAK.KO-12.0250	2차년
9	FIDO -제11부- 용어 해설	TTA (한국)	채택	김수형	TTAE.OT-12.0017-Part11	3차년
10	FIDO -제10부- 보안 참조	TTA (한국)	채택	김수형	TTAE.OT-12.0017-Part10	3차년
11	FIDO AppID와 Facet 규격 v1.0	TTA (한국)	채택	김수형	TTAE.OT-12.0017-Part9	3차년

나. 국제 표준화 성과

순번	표준명	발행기관(국)	채택여부	제안자	주요내용	발생차년
1	Web Certificate API 표준 초안	W3C (미국)	채택	조상래	액티브 X 이용 없이 웹브라우저에서 인증서 관리(발급/갱신/폐기) 기능을 제공하는 기술	1차년
2	Web Certificate API 표준 수정안	W3C (미국)	채택	조상래	인증서 관리 API 업데이트 및 서버와 교환하는 메시지 형식을 정의하는 기고서	1차년
3	Digital Certificate and Beyond	W3C (미국)	채택	조상래	인증서의 편의성과 보안성 높이기 위해 시도한 기술들을 소개함	2차년

4. 기술이전

순번	기술이전 내역	대상국명	대상기관명	계약체결일	당해년도 징수액 (백만원)	발생차수
1	스마트채널3 및 개인정보 추출 모듈	한국		2013.12.11	15	1차년
2	스마트채널3 및 개인정보 추출 모듈	한국		2013.12.11	30	1차년
3	웨어러블 장치를 이용한 거래내역확인 및 휴대폰인증 기술	한국		2013.12.20	30	1차년
4	터치사인	한국		2014.04.29	40	2차년
5	터치사인	한국		2014.08.07	50	2차년
6	터치사인	한국		2014.09.15	60	2차년
7	터치사인	한국		2014.11.07	60	2차년
8	스마트인증 및 개인정보탐지 모듈	한국		2014.07.11	105	2차년
9	비정상 DB 쿼리 탐지 기술	한국		2015.05.13	30	3차년
10	오프라인 간편결제 및 간편인증 기술	한국		2015.03.09	120	3차년
11	오프라인 간편결제 및 간편인증 기술	한국		2015.03.12	60	3차년
12	오프라인 간편결제 및 간편인증 기술	한국		2015.03.30	20	3차년
13	오프라인 간편결제 및 간편인증 기술	한국		2015.05.18	120	3차년
14	오프라인 간편결제 및 간편인증 기술	한국		2015.05.19	40	3차년
15	오프라인 간편결제 및 간편인증 기술	한국		2015.05.20	160	3차년
16	오프라인 간편결제 및 간편인증 기술	한국		2015.07.13	53	3차년
17	오프라인 간편결제 및 간편인증 기술	한국		2015.07.22	20	3차년

18	오프라인 간편결제 및 간편인증 기술	한국		2015.08.17	240	3차년
19	오프라인 간편결제 및 간편인증 기술	한국		2015.09.23	60	3차년
20	오프라인 간편결제 및 간편인증 기술	한국		2015.10.16	40	3차년
21	오프라인 간편결제 및 간편인증 기술	한국		2015.11.10	40	3차년
22	오프라인 간편결제 및 간편인증 기술	한국		2015.12.07	60	3차년
23	오프라인 간편결제 및 간편인증 기술	한국		2015.12.02	40	3차년
24	오프라인 간편결제 및 간편인증 기술	한국		2015.12.31	20	3차년

주 의

1. 이 연구보고서는 한국전자통신연구원의 주요사업으로 수행한 최종연구결과입니다.

2. 이 보고서의 내용을 발표할 때에는 반드시 한국전자통신연구원에서 수행한 주요사업 결과임을 밝혀야 합니다.