2014년 12월

14ZS1200-01-1412P

10

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, 모바일 환경에서 안전하게 사용할 수 있는 공인인증서 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.

2014 년 12 월

한국전자통신연구원 원장 김 흥 남

제 출 문

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

2014 년 12 월

주관연구기관 : 한국전자통신연구원

연구책임자 : 책임연구원 진승헌

연구참여자 : 책임연구원 조현숙

책임연구원 조진만

책임연구원 조영섭

책임연구원 최대선

책임연구원 조상래

책임연구원 노종혁

선임연구원 김수형

선임연구원 김승현

선임연구원 김석현

공동연구기관 : (주)비씨카드

연구책임자 : 책임연구원 장석호

연구참여자 : 책임연구원 이상우
선임연구원 김윤경
선임연구원 김명석
선임연구원 김원용
선임연구원 김철홍
책임연구원 권삼의

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 진행되며 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 조합 리스크 분석 기술 개발

다. 3차년도(2015년) : 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

Ⅳ. 연구결과

2014년 본 과제의 수행을 통하여 확보된 주요 연구개발 결과는 아래와 같다.

○ 핸즈프리 결제 시스템 개발
  • 비컨을 이용한 체크인 zone을 사용자 스마트폰이 인식하여 사용자 식별정보 노출 없는 안전한 체크인 및 핸즈프리 결제 시스템 구현
○ 메모리해킹 피싱 공격 방지 기술
  • 온라인 환경에서 사용자가 소지한 휴대폰 또는 현금카드(스마트카드)를 이용하여 피싱 공격으로부터 안전하게 전자서명 가능한 NFC 기반 인증서 관리 및 이용 기술 구현
○ 개인정보 조합 리스크 분석 기술 개발
  • SNS 등 단문 텍스트에서 개인정보를 추출하고 개인정보의 소유자를

식별하여, 주체별 개인정보에 대한 연결/조합을 통한 위험도를 제시하는 기술

○ 논문
- 국제 논문 1건 게재
- 국내 논문 10편 게재

○ 특허
- 국제 특허 5건 출원
- 국내 특허 6건 출원, 1건 출원 중

○ 표준화
- 국제 표준 기고서 1건 채택
- 국내 표준안 1건 채택

○ 기술이전
- 기술이전 5건 완료

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

○ 미개척 분야인 시큐리티 큐레이션과 개인정보 유통 보안 기술 개발을 통해 관련 모바일 서비스 기술 분야에서 세계 최고의 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 맞춤형/지능형으로 고도화하기 위한 기반기술로 활용될 것임

다. 사회적 측면

- ○ 온오프라인 피싱/사기, 개인정보 유출 등의 범죄 피해를 경감시킴
- ○ 개인정보 제공과 활용 동의에 대한 기존 절차를 최소화/간소화하며, 개인정보 활용이 필요한 모든 온오프라인 서비스와 산업분야에 활용 예상
- ○ 온라인과 오프라인 환경에서 사용자 스스로 자기결정권을 가지고 정보를 공유 · 제어할 공통 기술로 활용 예상

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 security 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 phishing attack prevention technology
- Development of personal information combination 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 personal information curation technology

○ Development of personal information inference risk analysis technology

Ⅳ. RESULTS

In 2014, the main outcome produced by performing the project are as follows.

○ Development of Hands-Free payment system

- Developed secure check-in and payment system without exposing personal information using a user smart phone that recognizes the check-in zone created by beacons

○ Development of defense technology against memory hacking phishing attacks

- Developed secure digital signature enabled NFC based certificate management and usage technology using mobile phone or credit card in online environment against memory hacking phishing attacks

○ Development of personal information open risk analysis technology

- Developed the technology that estimates the degree of risk

regarding connected and combined personal information and identifies an owner of personal information by extracting unstructured personal information disclosed in SNS as a form of short text

- ○ Papers
  - International - 1 published
  - Domestic - 10 published
- ○ Patents
  - International - 5 patented
  - Domestic - 6 patented and 1 proceeding
- ○ Standard
  - International contribution - 2 accepted
  - Domestic standard - 1 accepted

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 큐레이션[1]을 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

1) 시큐리티 큐레이션 : 온오프라인 거래에서 개인정보보호를 위해 리스크 분석, 피싱 방지, 보안 협상을 자동 수행

○ 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
- 광고, 추천, 타겟 검색 등 개인정보를 분석 활용하여 고부가 맞춤 서비스를 제공하고자 하는 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

○ 모바일결제 거래규모가 “해당부분은 한국전자통신연구원에서 저작권을 확보하지 못하여 공개대상에서 제외되었습니다”

○ ‘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 이용자 중심 고부가 서비스로 진화하기 위해 반드시 필요한 기술임

제 2 절 국내외 관련 기술의 현황

1. 국내외 기술 및 표준화 현황

2. 국내외 시장 현황

3. 국내외 경쟁기관 현황

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

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

[그림 1-4] 기술적 파급 효과

2. 경제적 산업적 측면

○ 개인정보 관리 분야의 시장규모는 “해당부분은 한국전자통신연구원에서 저작권을 확보하지 못하여 공개대상에서 제외되었습니다”

○ 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 맞춤형/지능형으로 고도화하기 위한 기반기술로 활용될 것임

[그림 1-5] 경제적 산업적 파급 효과

3. 사회적 측면

○ 온오프라인 피싱/사기, 개인정보 유출 등의 범죄 피해를 경감시킴

○ 개인정보 제공과 활용 동의에 대한 기존 절차를 최소화/간소화하며, 개인정보 활용이 필요한 모든 온오프라인 서비스와 산업분야에 활용 예상

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

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 • 온오프라인 피싱 방지 기술 • 개인정보 (노출, 연결, 추론) 리스크 분석 기술 • 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 • 개인정보 리스크 분석 기술

구분	내용
	○ 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 • 광고, 추천, 타겟 검색 등 개인정보를 분석 활용하여 고부가 맞춤 서비스를 제공하고자 하는 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

- 비콘 프리 핸즈프리 지불 기술
- 메모리해킹 피싱 공격 방지 기술
- 개인정보 조합 리스크 분석 기술
- 개인정보 (ID, 인증정보, 결제정보) 유통 보안 시스템 기술

○ 관련 정부기관, 산업체, 유관기관, 학계와의 연구협력(공동연구, 위탁, 용역)을 통하여 요구사항 도출, 시나리오 검토, 서비스 연계, 프로토타입 시스템 개발 등을 함께 추진함

- (주)비씨카드와 표준 POS 테스트베드 구축 및 스마트결제 응용서비스 개발
- 미래부/KISA/MOIBA와 공인인증서 정책, 기술개발 요구사항 협의 및 국제 표준화 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

○ 개인정보보호관련 법/정책 전문가를 활용하여 개인정보 조합 및 재식별 공격, 안티피싱 기술의 취약성을 분석하여 대응방안을 마련하고, 거래 안전을 위한 도구와 모델을 연구함

○ 유관기관 등을 활용해 산업계 현황과 상용화 시기 등을 파악하며 기술수요와 시나리오 검토 등을 수행함

○ 전년도 연구개발 결과 및 당해연도 개인정보 유통 보안 시스템 기술은 국내외 표준화 단체(W3C, TTA 등)를 통해 표준화 추진함

○ 사용자 인터페이스 및 응용서비스 시스템 개발 등은 공동연구기관, 전문업체 등에서 기 확보하고 있는 기술들을 활용, 본 과제는 핵심기술 개발에 집중하여 개발기간을 단축함

3. 개발기술의 평가방법 및 평가항목

[표 2-2] 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	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

4. 정량적 성과 목표

[표 2-3] 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/(1)	/	7/8	/	/	10/11	2/8	1/2 (0.5/0.6)	3/24	50/52
2차년도 (2014년)	3/5	/	5/6(1)	/	2/(2)	8/11	2/2	2/6 (0.7/3.3)	3/11	50/54
3차년도 (2015년)	3/	/	5/	/	2/	8/	2/	2/ (1/)	3/	50/
합계	10/5(1)	/	17/14(1)	/	4/(2)	26/22	6/9(1)	5/8 (2.2/3.9)	9/35	150/106

* 2014.12.기준
* 특허 ( )는 현재 출원 중인 건수임
* 논문 ( )는 현재 제출 건수임
* 기술이전 ( )는 기술료임 (억원 단위)

제 2 절 연차 목표 및 평가 방법

1. 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

2. 평가 방법

가. 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

나. 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

제 3 절 연차별 개발 내용 및 개발 범위

1. 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

제 3 장 결과 및 향후 계획

제 3 장 결과 및 향후 계획

제 1 절 연차 연구개발 결과 및 계획

1. 연차 연구개발 추진 일정

[표 3-1] 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 (감수형) (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 : 5건 - 비SCI논문 : 9건 - 표준기고서 : 0건 - 기술문서 : 22건 - 기술이전 : 1.65억								- 시험절차서 - 시험결과서 - 국내특허: 2건 - 비SCI논문: 2건 - 표준기고서: 2건 - 기술문서: 32건 - 기술이전: 1.65억 - SW 등록: 11건					1,617,000	12.38

2. 연차 연구개발 추진 실적

[표 3-2] 연구개발 추진 실적

목 표	세 부 계 획	실 적	차이 (달성도(%))
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 6건 - 국내 특허 출원중 1건 - 국제 특허 출원 5건 ○ 논문 - SCI 1건 Conditional Accept - SCI 1건 제출 - 비SCI 국제 1건 게재 - 비SCI 국내 10건 ○ 표준화 - 국내 표준안 1건 채택 - 국제 기고서 1건 채택 ○ 기술이전 3.3억 ○ S/W등록 11건 ○ 기술문서 54건	100
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	100

목 표	세 부 계 획	실 적	차이 (달성도(%))
		인식 판별 방법 - 터치사인 온라인 시스템 구현 - 아이핀(i-PIN) 서비스에 대한 액티브 피싱 공격 - 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	

목 표	세 부 계 획	실 적	차이 (달성도(%))
		가이드 - 안드로이드 SSL 구축 가이드 - FIDO 인증장치 개요 - FIDO ASM 개요 - FIDO ASM 서비스 AIDL - channel-id - 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	

목 표	세 부 계 획	실 적	차이 (달성도(%))
		- 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 - 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	100

목 표	세 부 계 획	실 적	차이 (달성도(%))
		. 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	
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	100

목 표	세 부 계 획	실 적	차이 (달성도(%))
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)	100

3. 각 기관/기업별 추진 내역

가. 스마트결제/공유를 위한 단말 인터페이스 개발

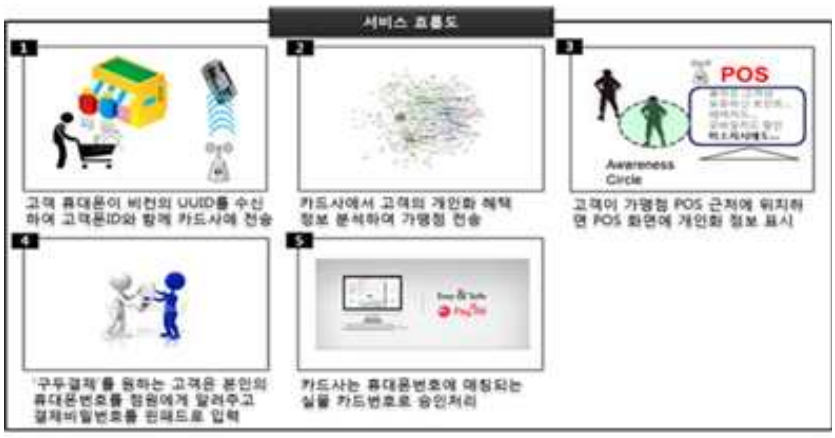
공동연구기관: (주)비씨카드

○ 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 3-1] 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 6건, 국내 출원 중 1건, 국제 출원 중 5건

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) 전자 신분증 시스템 및 이용 방법

7) 유사 사용자 식별 방법 및 그 이용 방법 (출원중)

8) Device and Method for providing security assistant service

9) Apparatus for verifying website and method thereof

10) Method, Apparatus, and system for using IC card as authentication medium

11) System and method for security authentication via mobile device

12) Mobile Terminal, Terminal And Authentication Method Using Security Cookie

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

: SCI 조건부게재승인 1건, SCI 심사중 1건, 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
12) Inferring Korean Residence Registration Numbers from Public Information on SNS, IEICE (SCI Conditional Accept)
13) Undisclosed Private Attribute Inference from Facebook Profile Data. ETRI Journal (SCI 제출)

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 3-2] 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 3-3] 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 3-4] 액티브X없는 터치사인

사. 기술이전

: 기술이전 6건 완료

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

- 1건: 쿠노소프트
- 1,500만원

2) 기술이전명: 터치사인

- 4건: 씽크풀, 시큐브, 한국디지털ID, SCE
- 21,000만원

3) 기술이전명: 스마트인증 및 개인정보 탐지 모듈

- 1건: 코나아이
- 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 3-5] 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 3-6] 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

입력날짜 : 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 본 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 '한O 인증서비스'에서 사용자 인증 및 이체 전자서명 목적으로 이용 중에 있다.

[그림 3-7] 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 3-8] 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 3-9] 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 3-10] 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 3-11] 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

입력날짜 : 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.

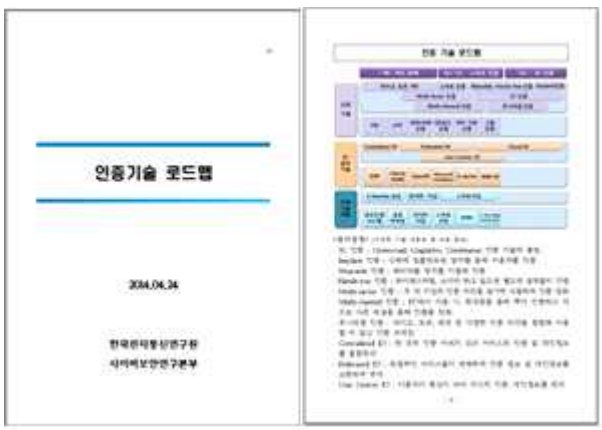
ETRI(한국전자통신연구원, 원장 김흥남)는 스마트폰을 이용한 안전한 인증 및 피싱 방지 기능을 제공하는 '스마트채널3' 기술을 개발했다고 23일 밝혔다.

[그림 3-12] 스마트채널3 보도 자료

카. 기술 동향 분석

1) 인증기술 로드맵

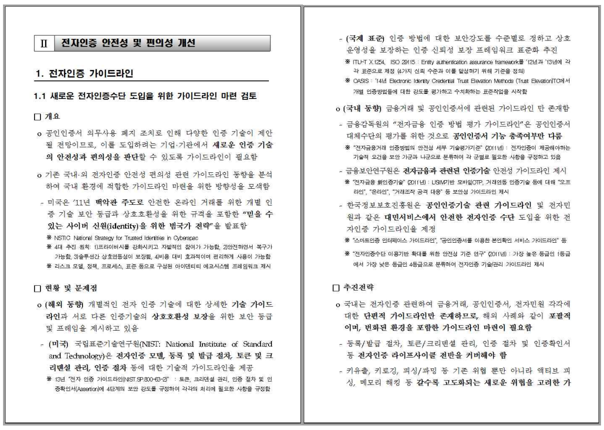
• 차세대 인증 기술 및 ETRI 보유 인증 기술 로드맵 작성
• 4월 24일 미래창조과학부 정보보호 정책과 보고



[그림 3-13] 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 상호운영성을 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 ElevationTC)에서 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**

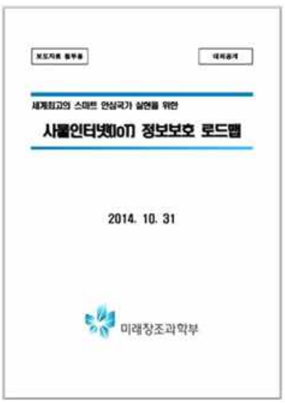
- 등록/발급 절차, 토큰/크리덴셜 관리, 인증 절차 및 인증확인서 등 **전자인증 라이프사이클 전반을 커버해야 함**

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

[그림 3-14] 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



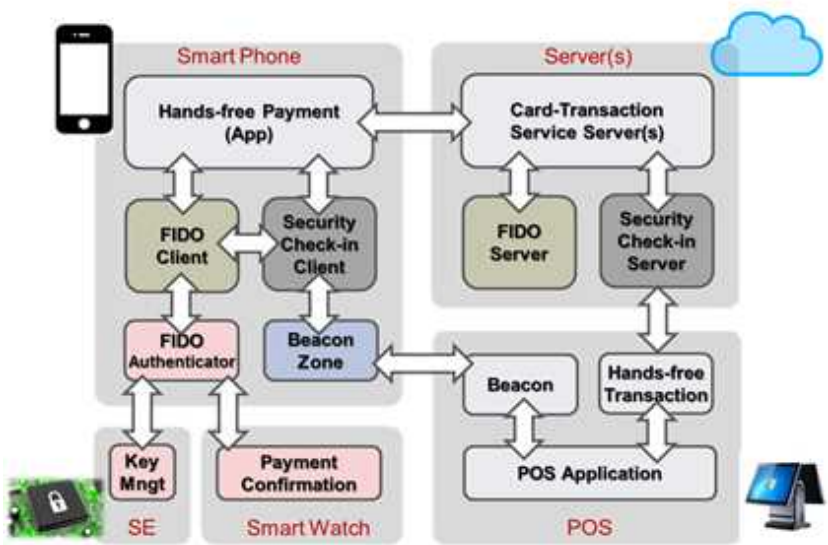
[그림 3-15] IoT 정보보호 계획

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



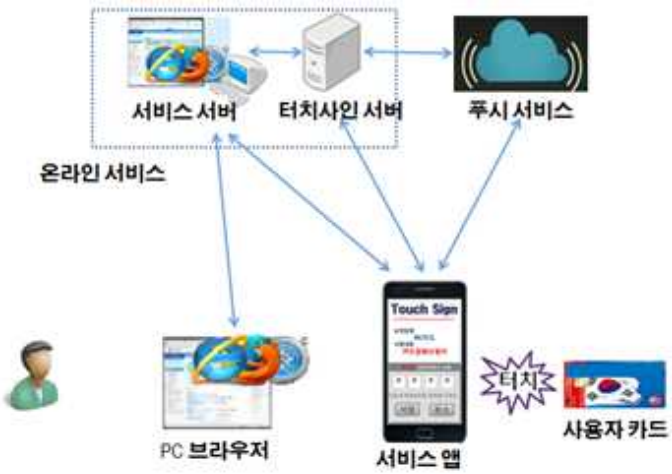
[그림 3-16] 핸즈프리 결제 시스템 구조도

[그림 3-17] 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



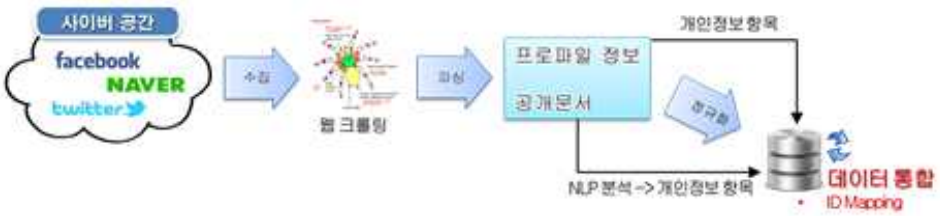
[그림 3-18] 터치사인 온라인 개념도

[그림 3-19] 터치사인 온라인 시연 화면

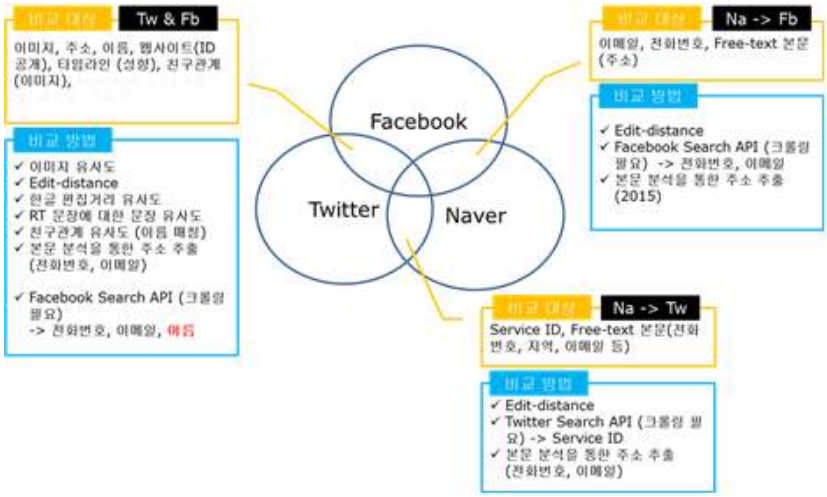
3) 개인정보 조합 리스크 분석 기술 개발

○ 개인정보 조합식별위험 분석 기술

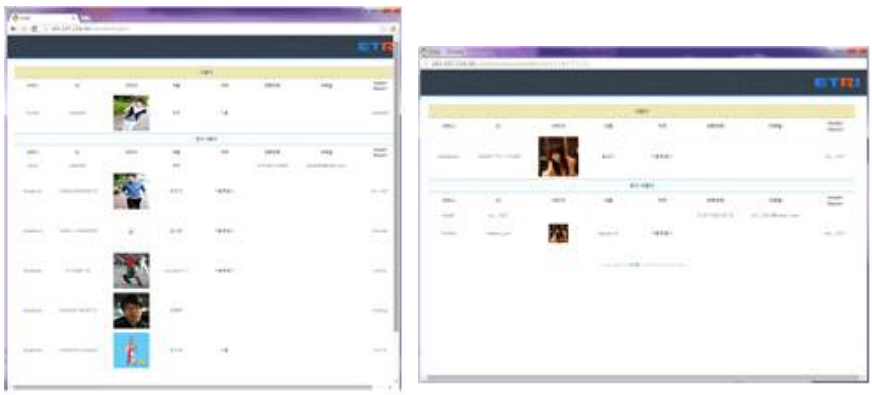
- 개발 내용
  - 공공 데이터 등 집적 데이터 및 SNS/웹사이트 등의 단문 데이터에서 개인정보를 추출하고, 해당 개인정보의 주체를 식별하여, 주체별 개인정보를 연결/조합을 통해 위험도를 제시
  - FB-TW-NA 3개 사이트 ID Mapping



[그림 3-20] 비정형 개인정보 탐지 및 조합 리스크 분석 시스템 개념도



[그림 3-21] ID Mapping 대상 및 연결 항목 예시



[그림 3-22] 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, 폭포, 계곡, 동굴)	(지명적으로 생성된 장소) 사람들이 모이는 곳
		LC_FACILITY	203	건물(지하철/기차역, 공항, 버스터미널, IC, 시장, 정류장, 단지, 항구, 건축물, 다리, 둑대, 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 3-32] 비정형 개인정보 태그 리스트

○ 개인정보 필터링 기술

- 개발 내용
  - TXT, HWP 파일의 개인정보를 탐지하여, 사용자 선택에 따라 마스킹하는 기술

제 2 절 시장 현황 및 사업화 전망

1. 시장 현황

가. 개인정보 유통 관련 시장 현황

○ 전세계 모바일 지불 시장의 규모는 2012년 2,020억 달러에서 2013년 4,100억 달러로 성장했으며, 2017년 까지 연평균 59% 성장하여 2조 달러 규모가 예상됨. 2013년 1억 6천만여 개의 NFC 지원 단말이 보급되었으며, 2017년까지 16억 7천여 개가 보급될 것으로 예상됨. NFC 지불이 모바일 지불에서 차지하는 비율은 2017년 20%를 차지하여 3,910억 달러 규모가 될 것으로 예상함[2)]

○ 2011년도 국내 휴대폰 결제시장 규모는 전년 대비 15% 증가한 2조 4,700억 원이며, 2012년에는 2억 8424억에 이를 것으로 예측됨[3)]

○ 애플과 페이팔 등이 발표한 블루투스 비콘(Beacon) 기술은 모바일 상거래의 핵심 기술로 사용될 전망이며, 2014년부터 2019년까지 6천만 개의 비콘 기기가 보급되어 1100억원 정도의 시장을 형성할 것으로 예측됨[4)]

나. 안티 피싱/파밍 시장 현황

○ 안티피싱 워킹그룹(APWG)에 따르면 2013년에는 492,300건의 피싱 공격(2012년 대비 80% 수준)으로 피해가 감소했으나, 2014년도 1분기는 125,215건으로 역대 2번째로 높은 공격 건수를 보임.[5)6)] 국내는 2013년도에 7,999건의 피싱 공격(2012년 대비 15.2% 증가)이 발생하였음[7)]

---

2) PortioResearch, Mobile Payments 2013-2017, http://www.portioresearch.com/en/major-reports/current-portfolio/mobile-payments-2013-2017.aspx
3) 전자신문, 2012/1/4, 2012년 휴대폰 결제 거래규모 2조8000억 원 넘어선다.
4) ABI Research, 2014
5) APWG, Phishign Activity Trends Report 4th Quater 2012, 2013.4
6) APWG, Phishign Activity Trends Report 1th Quater 2014, 2014.6
7) 인터넷진흥원, 인터넷 침해사고 대응통계, 2014.1

○ 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 X가드' 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

○ 국내 메모리 해킹 피해 규모는 560건(2013년부터 2014년 6월까지), 피해액은 26억 5000만원(2013년 6월부터 2013년 10월까지)에 달하며, 신종 피싱/파밍 공격에 따른 2013년도 피해규모는 704억 원에 달함[8)9)]

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

○ 전세계 빅데이터 시장은 2015년 390억 달러에서 2020년 760억 달러로 예측되며, 국내 빅데이터 스토리지 시장은 2014년 347억원에서 2018년 1,087억원으로 연간 31.3%의 성장을 예측하고 있음. 공공 IT 인프라를 포함한 국내 빅데이터 시장 규모는 2016년 3.3억 달러에서 2020년 8.9억 달러로 전망함[10)11)12)]

---

8) 금융감독원, 피싱사기 피해 구제현황 및 소비자 유의사항, 2014.2.25
9) 금융위원회, '신·변종 전기통신금융사기 피해방지 종합대책' 이행상황 점검, 2014.8.13
10) Market Info Group, 빅데이터 분석 전망 : 세계 시장 및 기술 예측, 2014
11) IDC 2014 자료를 아이뉴스24에서 재인용. 2014.11.19.

○ 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

- 안랩은 '애플리케이션 인텔리전스 서비스'를 통해 개인정보 유출 차단 서비스 제공
- 위너다임, 닉스테크 등은 기관 보유 개인정보를 스캔하여 마스킹하는 솔루션 제공
- 지란지교, 컴트루 테크놀로지, 이지서티, 유엠브이기술은 웹 게시물에 포함된 개인정보를 탐지하고 차단하는 필터링 솔루션 제공

12) KISTI, Market Report – 빅데이터 산업의 현황과 전망, 2013.4.

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 3-3] 국내외 여건 변화 및 대응 전략

세부 분야	국내외 여건 변화	대 응 전 략
정책적 여건	○ 공인인증서의 이용 불편과 인증서 유출 이슈가 사회적 현안 문제로 부각하여 관련 논의 및 정책 개발이 진행 중에 있음	○ 터치사인 기술의 기술이전, 추가 기술 개발, 시범사이트 구축 지원 • 미래부, 한국인터넷진흥원이 준비 중인 액티브X없는 공인인증서 시범사이트에 터치사인 적용을 위한 기술 지원
	○ 방통위는 '온라인 개인정보 취급 가이드라인'을 발표함. 서비스와 무관한 개인정보 수집 및 포괄적 동의 등 기존 관행에 제동, 또한 개인정보 보유기간 명확화를 추진함	○ 각 기관이 보유한 정형/비정형 개인정보의 탐지 및 중요도에 따른 유출 방지에 적용할 수 있도록 대응
기술적 여건	○ 아이폰 iOS7, 안드로이드 4.3 버전부터 BLE(Bluetooth Low Energy) 기능을 제공했으며, 2014년 하반기부터 관련 서비스의 본격 등장 예상됨	○ In-Store 환경에서 BLE 비콘 기반 체크인 및 결제 서비스를 제공하는 핸즈프리 결제 기술 개발
	○ 정상적으로 웹사이트를 사용하는 과정에서 해킹이 이루어져 사용자 계좌를 탈취하는 고도화 피싱/파밍 공격이 등장함	○ 별도의 신뢰 단말을 활용하여 거래의 무결성을 보장하는 터치사인 기술을 고도화하여 웹 환경에 연동함

세부 분야	국내외 여건 변화	대 응 전 략
	○ 빅데이터 환경 도래로 공공 분야의 데이터 개방 및 SNS 등 다양한 형태의 정보 공유가 시작되고 있음	○ 정보의 개방 및 공유에 따른 개인정보 노출 및 데이터 연결 등을 통한 민감정보 도출 가능성을 줄이기 위한 프라이버시 필터링 기술 개발 강화
표준화 여건	○ 카드사 등에서 고객정보 유출 방지, 업무효율성 제고 등을 위해 모바일기기를 이용한 전자발급 신청 시스템에 대한 관심 증가	○ 국내 표준화 단체를 통해 서비스 모바일기기에 전자서명을 제공하는 터치사인 기술의 표준화 추진 • TTA에 관련 표준안 (대면거래에서의 전자서명 규격) 제안 및 채택
	○ 미국 NIST를 중심으로 빅데이터 표준화 방향 정립이 진행중임	○ NBD-PWG(NIST Big Data – Public Working Group)에 참여하여 관련 표준화추진
사회적 여건	○ 온라인과 오프라인을 연계하는 O2O (Online to Offline) 비즈니스의 확대	○ O2O 비즈니스를 혁신할 차세대 IT기술로 각광받는 비콘(beacon)을 활용한 개인정보 유통보안 기술을 개발추진
	○ 인터넷 피싱/파밍에 대한 기술이 고도화 됨에 따라 사용자들의 불편함과 우려 확대	○ 사용자가 쉽고 안전하게 사용할 수 있는 UX와 보안기능에 초점을 맞춘 안티 피싱/파밍 기술을 개발
	○ 빅데이터를 활용한 프라이버시 침해 및 악용 사례가 지속적으로 증가하고 있음	○ 개발하는 빅데이터 프라이버시 보호 기술을 적극 보급하여, 침해 및 악용 등을 방지함에 따라 국민들에게 빅데이터 세상을 향유할 수 있는 기반 제공

3. 사업화 전망

- O 사용자 전자서명이 요구되는 전자입회신청서, 전자계약서 등의 서비스 단말에 사용자 스마트폰 또는 금융카드를 터치해 전자서명을 제공하며, 온라인 전자거래 시에도 터치만으로 사용자를 인증하는 터치사인 기술의 사업화 가능성 높음
- O 온라인과 오프라인을 연계하는 O2O(Online to Offline) 비즈니스가 점차 확대될 것으로 전망됨에 따라, 오프라인 사용자를 자연스럽게 온라인으로 연결해주는 비콘 기술 및 비콘 이용 시의 프라이버시와 보안 문제를 해결하는 기술 수요가 증가할 것으로 예상
- O 공인인증서 등을 대체하기 위한 국제 표준에 부합하는 인증 기술의 사업화 가능
- O 피싱/파밍 공격은 고도화(메모리해킹, 액티브피싱 등) 및 지능화(스미싱 등 다른 공격 기술 및 사회공학적인 방식과 접목)되는 추세이므로, 고도화 피싱/파밍의 공격을 분석하고 대응 방법을 선행적으로 연구하는 부분과 사용자의 편의성을 개선하는 부분의 수요가 꾸준히 증가할 것으로 예상
- O 개인정보 스캐닝/필터링 관련 업계에서는 비정형 개인정보 노출 탐지 및 데이터 연결 추론이 불가능하도록 하는 프라이버시 보호 기술이 부족함. 본 연구개발 결과는 바로 이 업계에서 필요로하는 기술로서, 기술 개발시, 기술이전을 통한 사업화 가능성이 높음

제 3 절 차기 연차 계획

1. 차기년도(2015년) 목표 및 내용

가. 연구개발목표

○ 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)
- 특허(국내/국제) 3/5건, 표준 2건, 논문(SCI/비SCI) 2/8건

나. 연구개발 내용

○ 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 4 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 3-4] 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 : 286.6%
○ 부채총계 21,676억원 / 자기자본총계 7,562억원</td></tr>
<tr><td>최근년도말 유동비율
(산식 : 유동자산/유동부채×100)</td><td colspan="3">○ 계산결과 : 117.05%
○ 유동자산 22924억원 / 유동부채 19,585억원</td></tr>
<tr><td>이자보상비율
(산식 : 영업이익/이자비용)</td><td colspan="3">○ 계산결과 : 913.1
○ 영업이익 1,461억원 이자비용 1.6억원</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>

부 록

부록

1. 특허

순번	특허명	출원 번호	출원국	출원일
1	모바일 인증 시스템 및 방법	2014-0003451	한국	2014.01
2	문자 인식의 후처리 방법 및 이를 이용하는 문자 인식 장치	2014-0008485	한국	2014.01
3	전자 서명 제공 장치 및 방법	2014-0014991	한국	2014.02
4	IC 카드를 인증 매체로 이용하기 위한 방법, 장치 및 시스템	2014-0065285	한국	2014.05
5	구역 기반의 사용자확인 시스템과 그 방법 및 구역 기반의 사용자확인 서버	2014-0117686	한국	2014.09
6	전자 신분증 시스템 및 이용 방법	2014-0152991	한국	2014.11
7	유사 사용자 식별 방법 및 그 이용 방법	PR20140849KR	한국	-
8	DEVICE AND METHOD FOR PROVIDING SECURITY ASSISTANT SERVICE	14/243081	미국	2014.04
9	APPARATUS FOR VERIFYING WEBSITE AND METHOD THEREOF	14/285253	미국	2014.05

순번	특허명	출원 번호	출원국	출원일
10	METHOD, APPARATUS, AND SYSTEM FOR USING IC CARD AS AUTHENTICATION MEDIUM	14/319412	미국	2014.06
11	SYSTEM AND METHOD FOR SECURITY AUTHENTICATION VIA MOBILE DEVICE	14/337881	미국	2014.05
12	MOBILE TERMINAL, TERMINAL AND AUTHENTICATION METHOD USING SECURITY COOKIE	14/516141	미국	2014.08

2. 논문

순번	논문 제목	학술지 명칭	게재연월	구분
1	터치사인 오프라인 전자서명 시스템 구현	대한전자공학회 하계종합학술대회	2014.06	비SCI
2	iBeacon 기술 동향 및 문제점 분석	한국컴퓨터종합학술대회	2014.06	비SCI
3	목표 문자열을 이용한 문자 인식 판별 방법	한국통신학회 하계종합학술발표대회	2014.06	비SCI
4	터치사인 온라인 시스템 구현	대한전자공학회 하계종합학술대회	2014.06	비SCI
5	아이핀(i-PIN) 서비스에 대한 액티브피싱 공격	대한전자공학회 하계종합학술대회	2014.06	비SCI
6	터치사인에서 인증서 관리 시스템 구현	대한전자공학회 하계종합학술대회	2014.06	비SCI
7	관계형 데이터베이스에서 준식별자를 이용한 익명화 처리 기법	한국정보보호학회 하계학술대회	2014.06	비SCI
8	패스워드 없는 인증기술 : FIDO	전자통신동향분석	2014.08	비SCI
9	다중 소셜 네트워크 서비스 간에 사용자 연결 방법	정보보호학회 논문지	2014.11	비SCI
10	온라인 중고물품판매에 대한 개인정보 노출 위협	한국정보처리학회 추계학술대회	2014.11	비SCI
11	Device Control Protocol using Mobile Phone	ICACT 2014	2014.02	비SCI

3. 표준화

가. 국내 표준화 성과

순번	표준명	발행 기관(국)	주요 내용	비고
1	대면거래에서의 전자서명 규격	TTA (한국)	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	TTAK.KO-12.0250

나. 국제 표준화 성과

순번	표준명	발행 기관(국)	주요 내용	비고
1	Digital Certificate and Beyond	W3C (미국)	인증서의 편의성과 보안성을 높이기 위해 시도한 기술들을 소개함	채택 완료

주 의

1. 이 연구보고서는 한국전자통신연구원의 주요사업으로 수행한 연구결과입니다.

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