ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

N-스크린 환경 내 신뢰할 수 있는 금융프레임워크 개발☆

Development of Framework for Trusted Financial Service in N-Screen Environment

김 경 진* 서 동 수** 홍 승 필***
Kyong-Jin Kim Dongsu Seo Seng-Phil Hong

요 약

스마트폰, 스마트기기 등의 기술 발전 및 확산은 기존의 IT 분야와 유관 산업이 접목하여 N-스크린 서비스를 제공하면서 이를 기반으로 한 금융거래 서비스가 빠르게 보편화되고 있다. N-스크린 서비스는 새로운 금융 서비스를 제공하는 전환점으로 국내에서도 정책 개선 및 기술향상을 위한 개발을 하고 있지만 아직 제공될 수 있는 금융 서비스의 인프라는 부족한 수준이며, 노출된 유·무선 네트워크 환경 내 역공학적인 측면에서도 민감한 금융정보 유출 및 개인정보의 위험 가능성이 나타나고 있다.

본 논문에서는 앞서 제시한 문제점의 해결방안으로 N-스크린 환경 내에서 금융 서비스에 대한 위협 및 취약점을 다각적 측면으로 분석하였으며, 이를 기반으로 안전한 금융 서비스를 제공할 수 있는 금융보안 프레임워크를 제안한다. 또한 제시한 프레임워크를 효과적으로 활용될 수 있도록 정책 및 기술적 설계방안을 통해 가능성을 타진한다.

ABSTRACT

With the spread of the new technologies like a smart phone, a smart pad, N-Screen service for financial transaction quickly became commonplace through the Internet. Although it has been developed related technologies and policies since the N-Screen has been provided in Korea, infrastructure for financial services is still lacking. It also has many potential problems including phishing or malware attacks, privacy information exposure & breaches, etc.

This work suggests the financial security framework in the side of information protection through threat · vulnerability analysis. Further, we examine the possibility of effective application methods based on political · technical design.

☞ keyword : Framework, Financial services, Privacy, Security, Vulnerability

1. 서 론

스마트 기기의 급속한 보급으로 PC, 전화 등 고정 플랫폼 위주의 금융거래가 스마트폰, 태블릿 PC, IPTV 등 다양한 전자적 기기의 융합을 기반으로 하는 지급 결제 규모가 급격히 증가하고 있다[1, 2]. 근접통신(NFC)서비스의 상용화, M-커머스, T-커머스 뿐만 아니라, 최근에는 태블릿 PC 기반의 뱅킹서비스가 개시되고 있으며 스마트TV에도 도입될 추세로 다양한 단말기에서 동일한 콘텐츠를 이용할 수 있는 N-스크린 서비스가 확산되고 있다. N-스크린은 사용자가 어떤 매체 및 단말에 관계없이 언제 어디서든 콘텐츠를 이용할 수 있는 것으로써, 여기서의 단말은 PC 뿐만 아니라 스마트폰, 스마트TV는 물론 향후 등장하게 되는 많은 기기를 대상으로 한다[2, 34].

이와 같이 전자금융 서비스는 다양한 형태 및 기기의 발전과 융합의 양상을 보이고 있지만[3], 새로운 기술발전에 따른 보다 지능화된 공격기술과 수많은 악성코드 등장으로 보안에 대한 우려도 높아지고 있다. 기존의 PC나 모바일 기반에서 제공되는 금융 서비스는 금융 보안 프로그램 취약점, 공인인증서 복제 및 유출 등 여전히 기술적 보안 위험에 노출되어 있다. 이러한 환경에서 스마트폰, 태블릿 PC, 스마트TV 등 N-스크린 서비스 확산은 불특정 다수의 접근이 용이한 개방형 네트워크를 이용하기 때문에 기존 장치 특성에 따른 금융 보안은 큰 의미가 없어졌다. 금융감독원에서는 '금융거래 시 지켜야 할 10계명 및 보안 대책', '스마트폰 전자금융 서비스 안전대책' 등을 지속적으로 연구·배포하고 있지만[4, 5], 현행

* 정 회 원 : 성신여자대학교 컴퓨터학과 박사수료
kyongjin@sungshin.ac.kr(주저자)
** 정 회 원 : 성신여자대학교 IT학부 교수
dseo@sungshin.ac.kr(교신저자)
*** 종신회원 : 성신여자대학교 IT학부 교수
philhong@sungshin.ac.kr
[2012/03/13 투고 - 2012/03/16 심사 - 2012/06/11 심사완료]
☆ 본 연구는 2011년도 서울시 산학연 협력사업(PA100040)의 지원을 받아 수행된 연구임

정책으로는 구체적인 대응방안이 어려운 실정이다.

본 연구는 다양한 매체 및 장치에 금융 서비스 도입이 확산됨에 따라 기존 전자장치에 대한 금융보안 정책 변화가 필요하다는 것을 인지하고, N-스크린 환경 내 금융 서비스 보안 정책 및 기술을 적용할 수 있는 프레임워크를 제시한다. 본 논문의 순서는 다음과 같다. 1장에서 간략한 연구 소개와 2장에서는 국내·외 관련연구를 통해 프레임워크를 분석한다. 3장에서는 N-스크린 상에서의 발생 가능한 금융 취약점 및 위험을 다각적 관점에서 제시하였고, 4장에서는 N-스크린 환경 내 신뢰할 수 있는 금융 프레임워크 제안 및 당위성을 기술한다. 5장에서는 프레임워크의 활용 및 적용방안으로써 정책적 설계 및 활용방안을 소개하였으며, 마지막으로 6장에서는 결론 및 향후 연구 방향을 논의한다.

2. 개인정보보호 프레임워크 사례 연구

(표 1)은 주요 표준화 프레임워크 사례연구를 정리한 것이다[6~18]. 여기서 프레임워크는 체계적인 개인·정보보호 대책 마련을 위해 상호 관련성이 있는 기술과 지식을 기반으로 연구된 것이다.

3. N-스크린 환경 내 금융 보안 고려사항

N-스크린 환경 내에서 금융 서비스 이용 시, 개인(민감)정보를 제공하는 매체의 환경 및 특성에 따라 다양한 취약점 및 위협요인이 발생하고 있다. 다음 (표 2)는 이러한 위협 요인 및 고려사항들을 요소별, 주체별, 위협 종류를 기준으로 분석하여 정리한 것이다[29].

4. N-스크린 환경 내 금융보안 프레임워크

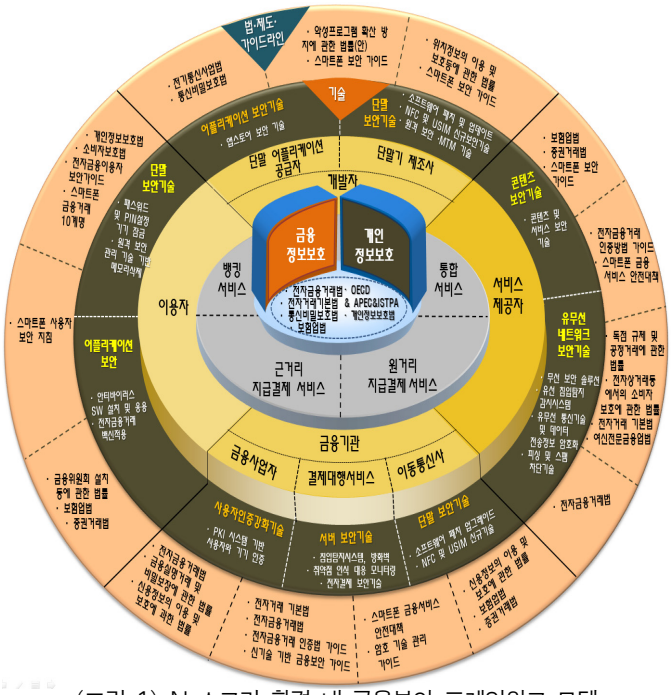
본 논문은 N-스크린 환경 내 금융보안 프레임워크를 제시한다. 프레임워크는 정보를 소유하고 있고 서비스를 이용하려는 이용자와 이용자에게 서비스를 제공하려는 제공자를 축으로 정보보호와 개인정보보호 영역을 나누어 구분한다. 또한 법·제도 대안을 마련하여 체계적인 인프라를 수립할 수 있도록 제시하고 있으며, 이를 기반으로 N-스크린 환경에 이용할 수 있는 기술적 대안을 설명한다. (그림 1)[29]은 금융 프레임워크 모델을 중점으로 세부적인 기능을 설명한다.

(표 1) 국내·외 (개인)정보보호 표준화 프레임워크 관련 요약

관련 프로젝트		연구 주제
모델	PISA	네트워크 환경에서 개인정보 유출 없이 사용자를 대신하여 복잡한 업무를 수행하는 지능형 소프트웨어 에이전트 모델 구축
프레임워크	PiMI	모바일 환경에서의 프라이버시 증대에 대한 기술적인 솔루션을 제안. 개인 데이터들의 개인정보보호 취약성을 해결하는 적절한 정보 보안과 개인 정보 보안 정책 구현을 제시
	PORTIA	특정 시스템 환경에서의 민감한 정보를 다루는 하나의 효과적이고 개념적인 프레임워크를 개발
	ISTPA	개인정보의 표준, 도구, 기술을 연구 및 평가하고 행정적, 기술적, 법적인 프레임워크 개발
	Safe Harbor Framework	EU 국가에서의 데이터 수집 사용 및 보유에 대한 표준으로 핵심은 적절한 개인정보보호 원칙을 확인하는 것
	APEC Privacy Framework	개인정보의 원활한 국제적 이전을 촉구하여 전자상거래를 활성화하는 동시에 개인정보 및 정보보호를 도모하기 위한 9가지 원칙
	The Val IT Framework	기업들이 정보기술투자의 가치를 인지하고 IT로 인한 변화를 실감할 수 있도록 돕는 일련의 검증된 사례를 수집해 묶은 지침서
개인정보 제어·관리	IBM's Tivoli	개인정보보호 정책에 의한 동적인 판단을 접근제어 방식을 통하여 규정하고 있는 것으로 민감한 개인정보의 접근을 관리하기 위한 솔루션
(개인)정보 확인 및 점검	IDMS	네트워크에 연결되는 개체의 Identity 속성, 신원증명서, 정보이용자격 등을 포함한 네트워크 Identity의 생명주기를 전체적으로 관리해주는 플랫폼 기반 구조
	RAPID	프라이버시와 신분관리(PIM)의 영역에서 다섯 가지 특수한 PIM 연구 목적을 지원하기 위해 만들어진 EU 프로젝트
	PRIME	통합된 Identity 관리 시스템들이 프라이버시를 강화하는 실제적 발전을 위한 설계 목적
	MIPA	일원화된 건강정보표준개발 촉진을 위해 개인정보기술과 프라이버시를 위한 인프라 구조 개발
	NTTCom	비밀정보 분산 기술에 의해 비밀성을 유지함으로써 안전한 개인 비밀정보의 저장이 가능하고 전자서명의 약점을 극복

(표 2) N-스크린 금융거래상의 개인(민감)정보 위협 및 고려사항 분석

요소	주체	위험 유형	위협 요인 및 고려사항
기술 측면	관리자	권한 관리 및 시스템 오류로 인한 개인정보 노출	-권한 관리자 또는 권한 관리 시스템의 오류 개인 정보 노출 -부주의한 권한 공유로 인해 권한이 없는 자의 개인정보 열람 및 이용
	사용자	커널을 통한 위협 노출	-개인화 과정에서 제공자가 제공하는 기본제공 보호 장치 해제
	제3자	시스템 해킹 및 DDoS 공격	-운영체제, 응용프로그램의 취약점을 악용한 시스템 해킹 공격 -네트워크 장비, 주요서버에 대한 DDoS 공격으로 방송 및 인터넷 서비스 마비
	개발자	플랫폼의 취약점을 이용한 유출	-플랫폼에 의도적으로 악성 코드 삽입하여 정보탈취 -기기들의 탈옥 도구로 가장으로 악성코드 배포로 인한 비밀번호 탈취
		통합인증 기술 부재	-사용자, 콘텐츠, 매체별 통합인증을 기반으로 하는 보안 인증 기술의 부재를 이용한 개인(민감)정보위협
관리 측면	관리자	불법유출 및 정보 미파기	-수집된 개인정보를 안전하지 못한 상태로의 저장 -고지한 개인정보 관리 이후에도 정보상태 유지
		부적절한 모니터링	-사용자 동의 없이 사용자의 활동이나 사생활의 모니터링
	사용자	개인인증 정보 유출/공유	-기기 내 인증정보 오픈 및 저장 - 타인에 의해 손쉽게 개인(민감) 정보 공개 -사용자 부주의로 인한 분실, 도난 개인정보 노출
	개발자	부주의한 문서 관리 정보유출	-단말 권한/취약점 상세 문서의 부주의한 관리로 제 3자 개인정보 접근 탈취 위협 -펌웨어 업데이트 및 보안 안전설치 홍보 부족
서비스 측면	관리자	맞춤형 서비스로 인한 개인정보 수집	-맞춤형 서비스 제공을 위한 과도한 정보 수집 -명시한 범위를 넘어선 이용 또는 제 3자 제공
		오류로 인한 개인정보 노출	-다양한 제휴서비스를 제공하기 위해 연동된 서비스 오류로 인한 개인정보 노출
	제3자	악성코드 유포	-앱스토어를 통한 악성코드, 바이러스 감염 파일 유포
		응용서비스 취약성 위협	-노출된 응용서비스취약점을 이용한 위협
	개발자	앱 스토어를 통한 개인정보 유출	-개발자 인증 체계 부재로 악성코드 배포 -오픈 마켓을 통한 자유롭게 제작 배포되는 어플리케이션에 대한 체계적 보안 검증체계부족
		개발가이드라인 및 표준 부재	-보안이 고려된 다양한 플랫폼 환경 내 개발 가이드라인 및 표준 기술의 부재로 인한 취약점 증대
법·제도 측면	관리자	권한 관리를 이용한 개인정보 불법유출 및 판매	-서비스 제공자의 개인정보 관리에 대한 적합성을 평가받기 위한 관련 제도 미비 -서비스 중단 및 오류에 대한 책임, 수탁자 관리 감독 책임 등의 요구 부족 -신규기술 및 융합 서비스 환경에 적합한 완전한 규율의 어려움
	제3자	해킹,공격을 통한 사용자정보위협	-개인(민감)정보 노출 및 유출시 일원화된 법적 기준 부재
	이용자	분실 및 개인정보 위협	-다매체 도난 및 분실로 인한 개인(민감)정보 유출에 대응하는 법. 제도적 부재
	개발자	부주의한 관리 및 개인정보 노출	-개발소스코드에 대한 인증 및 소프트웨어 코드서명에 대한 책임부여에 대한 법적 규제 부재 -취약점 노출로 인한 책임과 의무 법 미비
인식·윤리 측면	관리자	관리자의 보안의식 부족	-권한관리에 대한 시스템 체계와 규제 체계 부재 -사회공학적 공격을 예방하기 위한 보안인식 부족
	사용자	개인의 정보관리 인식부족	-연령별 개인의 정보관리 및 처리 방법에 대한 인식교육 부족 -신규 융합서비스 등장 시 발생 가능한 위험 정보 공지 및 예방 교육의 미흡
	개발자	사명의식 부족	-소프트웨어/하드웨어 개발에 대한 사명의식 동기를 부여하고 코드, 취약점 문서관리교육 미흡



(그림 1) N-스크린 환경 내 금융보안 프레임워크 모델

4.1 프레임워크의 당위성

프레임워크의 당위성을 설명하기 위해 금융정보 서비스 관련 법률, 개인정보와 관련된 OECD 8가지 원칙 등의 가이드라인, 그리고 ISTPA, PISA와 같은 국외 정보보호 프레임워크 프로젝트 등을 참고하였으며, (표 3)은 프레임워크 구성에 따른 내역과 각 내역에 해당하는 참고자료를 나타낸 표이다.

4.2 프레임워크의 구성요소

4.2.1 주체별

프레임워크의 금융 서비스는 스마트폰에 이어 스마트패드가 크게 확산하면서 여러 타산업과 접목시켜 서비스가 영역을 확장하면서 신규 서비스를 제공하기 시작했다. 주요 은행들의 경우 스마트 금융 서비스 계획을 추진 중이고, 보험사도 기존의 기본적인 업무뿐만 아니라 입출금, 보험 가입 등 서비스를 확대해 모바일 기기 등을 활용한 스마트 금융 서비스를 제공하고 있다[21]. 금융서비스의 대표적 서비스인 뱅킹은 N-스크린 기반의 다양한 기기들을 이용하여 은행의 자금이체 뿐만 아니라 증권, 보험, 외국환 거래 등 다양한 분야에서 금융 업무를 이용한다. 또한 뱅킹뿐만 아니라, 점차 선불충전 기반의 소액지급 및 지로납부나 모바일 전자상거래 등이 가능해지면서 다양한 지급결제 서비스가 시도되고 있다. 특히 직접 사람과의 거래하는 근거리 지급결제는 카드기반의 서비스를 휴대폰에 적용한 것이고, N-스크린 기반의 스마트기기를 통해서하는 온라인 상거래는 인터넷 및 SMS 기반 원거리 지급결제를 한다. 이를 기반으로 본 논문에서 (표 4)와 같이 서비스를 구분하여 운영상 보안 요구사항을 마련한다.

4.2.2 서비스별

금융 서비스는 스마트폰에 이어 스마트패드가 크게 확산하면서 여러 타산업과 접목시켜 서비스가 영역을 확장하면서 신규 서비스를 제공하기 시작했다. 주요 은행들의 경우 스마트 금융 서비스 계획을 추진 중이고, 보험사도 기존의 기본적인 업무뿐만 아니라 입출금, 보험 가입 등 서비스를 확대해 모바일 기기 등을 활용한 스마트 금융 서비스를 제공하고 있다. 금융서비스의 대표적 서비스인 뱅킹은 N-스크린 기반의 다양한 기기들을 이용하여 은행

(표 3) 참고자료에 의한 프레임워크의 당위성

	주요내역	법제도 및 기술관련	프레임워크
주체별	-금융기관 -서비스 제공자 -개발자 -이용자	-금융실명거래 및 비밀보장에 관한 법률[19] -전자금융거래법[20] -정보통신정책연구원[26, 28] ✓ 모바일 지급결제동향과 서비스 활성화를 위한 시사점 논의 ✓ 인터넷기반산업의 지불결제 서비스 시장 구조 및 전망	-The Val IT Framework -MIPA -IDMS [11, 13, 16]
서비스별	-뱅킹 서비스 -근거리 결제서비스 -원거리 결제서비스 -통합 서비스	-지식경제부 기술 표준원 금융서비스 현황[18] ✓ 모바일 지급결제 표준화 및 기술 ✓ 모바일 단말 전자결제 서비스 활성화 방안 -TTA 표준화전략 로드맵 “모바일 서비스” 분야[30]	-ISTPA -The Val IT Framework -IBM's Tivoli [8, 11, 12]
법·제도적·가이드별	-법제도 ✓ 전자금융거래법 ✓ 전자거래기본법 ✓ 개인정보보호법 -가이드라인 ✓ 전자금융관련가이드	-금융거래 관련법률[19, 20] -금융보안연구원[23] ✓ 금융부문 암호기술 관리 가이드 -금융감독원[4, 5, 18, 24] ✓ 금융거래 10계명 마련 ✓ 스마트폰 전자금융 서비스 안전대책	-OECD -PRIME -Safe Harbor Framework -APEC Privacy Framework -PORTIA [7, 9, 10, 15]
기술별	-서버 보안 -유·무선 네트워크 보안 -단말 보안 -사용자 인증강화 -어플리케이션 보안	-TTA 및 ETRI 정보보호 관련 기술 [31, 32, 33] ✓ 정부산하기관의 정보보호 표준화 기술 ✓ Privacy on the Web: Facts, Challenges, and Solutions -금융보안연구원 가이드라인[23, 24, 25] ✓ 금융부문 스마트폰 보안 가이드 ✓ 금융부문 무선랜 보안 가이드	-RAPID -MIPA -PISA -PiMI -PORTIA -PRIME -IBM's Tivoli [6, 7, 12, 14, 15, 16]

(표 4) 주체별 정의

주체	세부 주체	역할	해당 업종	보안 고려사항
금융기관	금융서비스 사업자	-금융업 및 관련 업무를 행하고 이용자에게 서비스를 제공 -이용자의 계정 발급 및 유지관리, 거래내역 데이터베이스 확보	은행,카드회사, 증권사 등	✓ 인증기능 강화 ✓ 개인 및 결제 정보를 암호화 / 보안 기능 제공 ✓ 이동통신사는 기기에 제공되는 어플리케이션 검수를 강화
	결제대행 서비스사업자	-금융 일부 업무를 대행하는 자 -기기로부터의 데이터를 은행 및 지급결제 네트워크에 전송 및 처리	PG/모바일 결제 (다날, 모빌리언스)	
	이동통신사	-금융 서비스 이용정보, 결제확인 및 지급 정보 등을 제공 -이용자 정보를 활용하여 부분적 지불결제 서비스 제공	통신업체(SKT, KTF, LGT)	
서비스 제공자	거래서비스 제공자	-결제를 통해 콘텐츠 및 서비스를 판매하여 직접적으로 이용자에게 서비스를 제공	콘텐츠사업자, 온오프라인 상점	✓ 콘텐츠 안전성 강화
개발자	단말 어플리케이션 공급자	-서비스 이용을 위해 단말에서 작동되는 소프트웨어나 어플리케이션을 제공	어플리케이션 개발자	✓ 하드웨어 및 소프트웨어 측면에서 기기 보안성 강화
	단말기제조사	-N-스크린으로 이용할 수 있는 단말기 제조 공급자	업체 (삼성, LG, 애플 등)	
이용자	서비스이용자	-전자금융거래를 하거나 서비스를 이용하는 자	소비자, 금융고객	✓ 보안패치 설치 및 업그레이드

의 자금이체 뿐만 아니라 증권, 보험, 외국환 거래 등 다양한 분야에서 금융 업무를 이용한다. 또한 뱅킹뿐만 아니라, 점차 선불충전 기반의 소액지급 및 지로납부나 모바일 전자상거래 등이 가능해지면서 다양한 지급결제 서비스가 시도되고 있다. 특히 직접 사람과의 거래하는 근거리 지급결제는 카드기반의 서비스를 휴대폰에 적용한 것이고, N-스크린 기반의 스마트기기를 통해서하는 온라인 상거래는 인터넷 및 SMS 기반 원거리 지급결제를 한

(표 5) 이용 서비스 분류

서비스	해당 분야	역할
뱅킹 서비스	-스마트폰 뱅킹 -스마트패드 뱅킹 -TV 뱅킹 등	-은행 업무 ✓ 거래기능 : 계좌개설, 계좌이체, 납입, 카드결제 등 ✓ 조회기능 : 예금/적금/카드, 대출, 신용카드, 환율, 수표 등
근거리 지급결제 서비스	-비접촉식 오프라인 결제 서비스 -공공재 거래 서비스	-스마트칩 또는 USIM 장착으로 단말 서비스 제공 ✓ 칩을 통해 카드 가맹점/인터넷 쇼핑몰에서 오프라인 결제 ✓ 교통카드기능 서비스 제공 -스마트기기에 쿠폰 제공 ✓ 위치기반서비스로 근거리에 위치한 가게의 쿠폰 제공 -NFC로 양방향 서비스 제공 ✓ 스마트기기를 통해 사업자들은 다양한 부가서비스를 제공하고 마케팅 효과 증대
원거리 지급결제 서비스	-송금서비스 -상거래 서비스 -E-commerce -M-commerce -T-commerce -소액결제 서비스	-가상계좌 송금 서비스 ✓ 이동통신사와 같은 은행에 개설한 가상계좌를 이용하여 휴대폰 송금 서비스나 대금결제 서비스를 제공 -소액결제 서비스 ✓ 스마트기기를 통해 물품 구입 시 모바일 이용요금에 합산하여 결제 및 지불하는 소액결제 서비스 -인터넷 및 네트워크를 이용한 상거래, 티켓 예매 ✓ 스마트기기를 통해 온라인 쇼핑몰에서 디지털 컨텐츠 및 제품 등 구매 -소셜커머스를 통해 쿠폰 제공 ✓ 일정 수 이상의 구매자가 모이면 할인가로 상품을 제공
통합 서비스	-증권 서비스 -보험 서비스 -주식 서비스	-증권, 보험 등 다양한 분야를 이용한 통합금융 ✓ 주식현재가 조회 및 주식거래 ✓ 고객에 맞는 보험 설계 및 청약 서비스, 보험상품구입 ✓ 증권매매와 펀드거래

다. 이를 기반으로 본 논문에서 (표 5)와 같이 서비스를 구분하여 운영상 보안 요구사항을 마련한다.

4.2.3 법・제도・가이드라인별

방송과 통신이 융합된 서비스의 확장으로 다양한 매체를 일관성 있게 규제하고 발전시키기 위해서는 산발적으로 제정되고 있는 법적 규제의 체계화가 필요한 실정이다. 특히 기동성, 휴대성, 편의성을 기반으로 하는 이기종 다매체 사이에서 빠르게 급증하는 다양한 지급 관련 서비스 어플리케이션들은 개인(민감)정보를 적극 활용 가능한 기술 상태에 놓여져 있다고 하겠다. 특히, 개인(민감)정보는 전자식 금융결제를 위한 필수 불가결 요소로써 다양한 이기종 매체를 이용시 언제, 어디서든 접근 가능한 위험에 노출되어 있다. 이에 따라 다양한 매체별(N-스크린) 기밀성, 무결성, 가용성이 고려된 법, 제도, 가이드라인 [19~28]이 적극 활용되어져야 할 것이다. 본 논문에서는 전자금융거래를 이용 및 활용하고자 하는 세부 주체자별 관련 법, 제도, 가이드라인을 분류함으로써, 주체별로 가지는 역할별 의무절차 및 규제의 명확성을 위해 아래의 (표 6)을 마련하였다.

4.2.4 기술적 방안

스마트기기 기반의 금융 서비스에 대해서는 지원기술에 따라서 보안적용을 한다. 스마트기기의 특성상 무선 네트워크 및 인터넷에서 이용하여 전송되는 데이터 및 정보를 보호해줄 수 있는 무선보안과 함께 무선 인터넷 망과 IP 백본망과의 연동망 구간에 네트워크 침입탐지 및 대응시스템 구축하는 등 보안이 강화되어야 한다. 또한, N-스크린 환경 내 스마트기기의 금융서비스 특징을 기반으로 단말 내 설치하는 VM(Virtual Machine) 방식 등에 대해서도 기술적 보호 대책이 필요하다. ((표 7) 참조)

5. 금융보안 프레임워크 활용방안

제시한 프레임워크를 기반으로 금융 서비스의 보호 마련을 위해 N-스크린 금융서비스의 활용단계와 이를 축으로 하여 금융 서비스 활용단계, 개인정보 활용단계로 전체적인 개요를 제시한다. 개인정보 활용단계는 개인정보 및 인증 및 거래 중요정보가 이용되는 N-스크린 환경에서 정책 및 지침, 절차, 가이드라인을 준수하여 생명주기

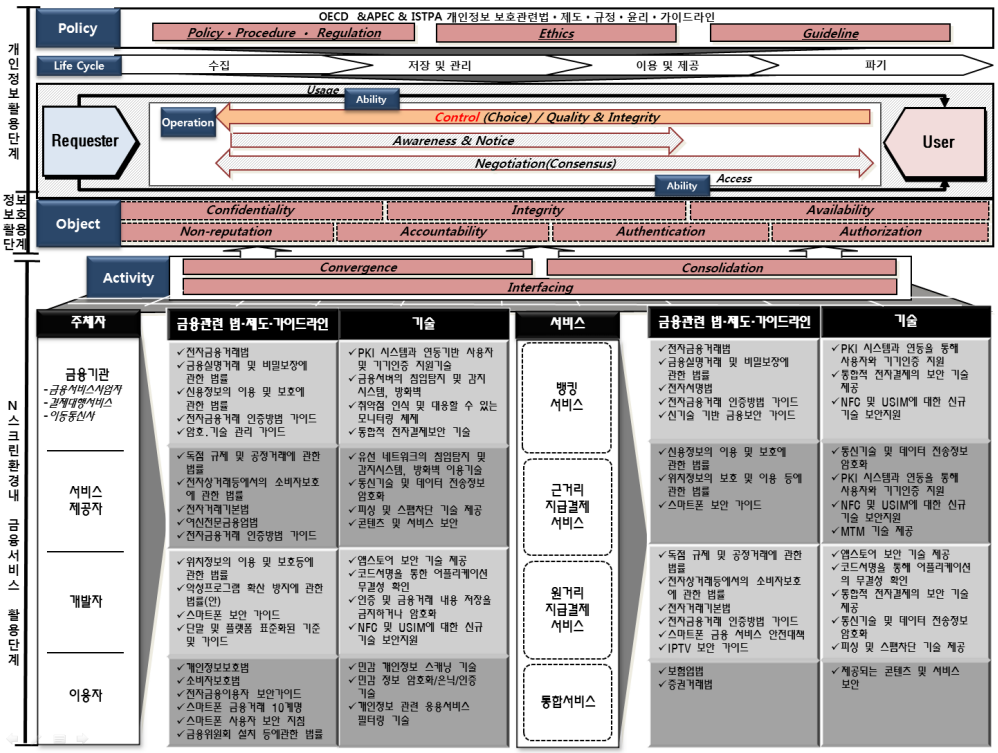
(표 6) 역할별 국내 법, 제도, 가이드라인 분류

주체	세부주체	개인(민감)정보보호 관련 법	개인(민감)정보보호 가이드라인
금융기관	금융 서비스 사업자	-전자금융거래법 -금융실명거래 및 비밀보장에 관한 법률 -전자서명법	-DB보안 가이드 -전자금융거래 인증방법 가이드 -금융 클라우드 컴퓨팅 보안가이드 -신기술 기반 금융보안 가이드
	결제대행 서비스 사업자	-정보통신기반보호법 -통신비밀보호법 -신용정보의 이용 및 보호에 관한 법률	-VoIP 보안 가이드 -암호·기술 관리 가이드 -무선랜 보안 가이드
서비스 제공자	거래 서비스 제공자	-독점 규제 및 공정거래에 관한 법률 -전자상거래등에서의 소비자보호에 관한 법률 -전자거래기본법 -여신전문금융업법	-금융 클라우드 컴퓨팅 보안가이드 -응용서비스 인증마크제도 -전자금융거래 인증방법 가이드 -스마트폰 금융 서비스 안전대책
개발자	단말 어플리케이션 공급자	-전기통신사업법 -정보통신기반보호법 -위치정보의 이용 및 보호 등에 관한 법률	-응용서비스 인증마크제도 -방송통신 서비스 제공 안전 가이드라인
	단말기 제조사	-통신비밀보호법 -악성프로그램 확산 방지에 관한 법률(안)	-스마트폰 보안 가이드 -단말 및 플랫폼 표준화된 기준 및 가이드 -단말 및 플랫폼 보안성 검증 및 개발 가이드
이용자	서비스 이용자	-개인정보보호법 -소비자보호법	-전자금융이용자 보안가이드 -스마트폰 금융거래 10계명 -스마트폰 사용자 보안 지침

(표 7) 기술적 보호 대책

보안영역	보안요소	보안 대책	세부 보안 대책
무선 네트워크 (개방성)	근거리 무선구간 보안	통신구간 보안	-NFC에서 암호통신을 위한 공유 비밀 생성
		데이터 보안	-NFC에서 전송정보의 기밀성과 무결성 제공
		기기인증 기술	-스마트기기에 부여되는 칩 또는 고유한 번호를 통해 인증하는 방식
	원거리 네트워크 보안	통신구간 보안	-침입탐지 및 감지시스템/방화벽 등 설치 -통신경로상의 정보의 침해 사고 예방
		데이터 보안	-거래내용의 기밀성 및 무결성 보장
		Ad-hoc을 통한 접근통제	-보안위협으로부터 능동적으로 방어할 수 있는 네트워크 접근 제어
		사용자 및 기기인증 기술	-기기의 고유번호와 아이디/패스워드, 공인인증서를 통해 인증하는 방식
플랫폼 및 단말 (휴대성)	단말기기 보안	단말기 잠금 기능	-패스워드 및 PIN을 설정해 기기 전체에 대한 잠금 설정
		단말 내 저장 정보보호	-인증 및 금융거래 내용 암호화 또는 저장금지 -키/터치패드에 입력정보 보호기술을 적용
		분실 및 도난방지	-스마트기기의 부적절한 접근 시 메모리 삭제 -패스워드/PIN 입력을 실패하는 경우 삭제 -직접 초기화가 어려울 때 원격 삭제
	어플리케이션 개발 및 이용 보안	어플리케이션 안전성 검증	-코드 서명을 통해 어플리케이션의 변조검증 -오픈마켓에서 모니터링 체계 마련
		악성코드 예방대책 기술	-신규서비스의 스팸 위험성을 분석 -지능형 필터링 등 안티스팸 서비스 강화
		정기적인 S/W 업데이트	-전자금융서비스 이용 시 백신 적용 -중요 S/W 패치 및 업데이트 서비스 지원

단계를 수행하면서 개인정보를 안전하게 보호한다. 금융 서비스 활용단계는 N-스크린 환경 내 금융 서비스를 주체별로 구분하고 법·제도·가이드라인 대안을 마련하여 체계적인 인프라를 수립할 수 있도록 하며, 이를 기반으로 기술적 대안을 제공한다. (그림 2)의 프레임워크 상관관계는 금융 서비스 환경 및 시스템 분석을 통해 서비스 규모에 따라 다양한 상황 및 환경에서 실제 적용이 가능하도록 방안을 마련한다.



(그림 2) 금융보안 프레임워크 상관관계

(표 8) 주체별 정책 및 기술적 보호 방안

주체	서비스	적용보안 기술	법·제도·가이드라인
금융기관	뱅킹	-사용자 인증강화기술 -PKI 시스템과 연동을 통해 사용자와 기기인증 지원 -서버 보안기술 -침입탐지 및 감지시스템, 방화벽 등 설치 -취약점 인식 및 대응할 수 있는 모니터링 체제 구축 -통합적 전자결제의 보안 기술 제공	-전자금융거래법 -금융실명거래 및 비밀보장에 관한 법률 -신용정보의 이용 및 보호에 관한 법률
	원거리 지급결제		-전자거래기본법 -전자금융거래법 -전자금융거래 인증방법 가이드 -신기술 기반 금융보안 가이드 -무선랜 보안 가이드
	근거리 지급결제	-사용자 인증강화기술 -PKI 시스템과 내장칩의 연동으로 기기 인증 지원	-스마트폰 금융서비스 안전대책 -암호·기술 관리 가이드
	통합	-단말 보안기술 -금융거래 시 중요 S/W 패치, 업데이트 지원 -NFC 등 신규기술 보안지원	-신용정보의 이용 및 보호에 관한 법률 -보험업법 / 증권거래법
서비스 제공자	뱅킹	-유·무선 네트워크 보안기술 -무선랜 보안 솔루션 -유선 네트워크의 침입탐지 및 감지시스템, 방화벽 등 설치 -유·무선 통신기술 및 데이터 전송정보 암호화 -피싱 및 스팸차단 기술 제공	-전자금융거래법
	원거리 지급결제		-독점 규제 및 공정거래에 관한 법률 -전자상거래등에서의 소비자보호에 관한 법률 -전자거래기본법
	근거리 지급결제		-전자금융거래 인증방법 가이드 -스마트폰 금융서비스 안전대책
	통합	-콘텐츠 보안기술 -이용자에게 제공되는 콘텐츠 및 서비스 보안 기술	-보험업법 / 증권거래법 -스마트폰 보안 가이드

(표 8) 주체별 정책 및 기술적 보호 방안(계속)

주체	서비스	적용보안 기술	법 · 제도 · 가이드라인
개발자	뱅킹	-어플리케이션 보안기술 -앱스토어 보안 기술* 제공 단말 보안기술 -금융거래 시 중요 S/W 패치 및 업데이트 지원 -인증 및 금융거래 내용 저장을 금지하거나 암호화	-전기통신사업법 -통신비밀보호법
	원거리 지급결제		-위치정보의 이용 및 보호등에 관한 법률 -악성프로그램 확산 방지에 관한 법률 -스마트폰 및 IPTV 보안 가이드
	근거리 지급결제	-단말 보안기술 -NFC 및 USIM에 대한 신규기술 보안지원 -원격 보안관리 기술** 지원 -MTM 기술*** 제공 -패스워드 및 PIN 설정으로 기기 잠금 기술 제공	-스마트폰 보안 가이드 -응용서비스 인증마크제도 -단말 및 플랫폼 표준화된 기준 및 가이드 -단말 및 플랫폼 보안성 검증 및 개발 가이드
	통합	-어플리케이션 보안기술 -코드 서명을 통해 어플리케이션의 무결성을 확인	-위치정보의 이용 및 보호등에 관한 법률 -스마트폰 보안 가이드
이용자	뱅킹	-어플리케이션 보안기술 -안티바이러스 SW 설치 및 운용 -전자금융거래 백신 적용 -단말 보안기술 -패스워드 및 PIN 설정으로 기기잠금 이용 -원격 보안관리 기술 이용하여 메모리 삭제 ※ *보안인식고취*	-개인정보보호법 -소비자보호법 -전자금융이용자 보안가이드 -스마트폰 금융거래 10계명
	원거리 지급결제		
	근거리 지급결제		-스마트폰 사용자 보안 지침
	통합		-금융위원회설치 등에 관한 법률 -보험업법 / 증권거래법

5.1 프레임워크 기반의 금융보안 정책·설계

프레임워크에 제안한 정책 및 기술적 보안 대책은 본 논문에서 정의한 금융관련 주체별로 (표 8)과 같이 적용될 수 있다.

6. 결언 및 향후연구

N-스크린 환경 내 금융 서비스는 다양한 산업 및 분야로 영역을 확장하고 있는 신규 서비스로써 언제, 어디서든 다양한 어플리케이션을 통해 신속한 자금이체 및 거래가 가능하다. 하지만 이러한 신규 서비스 확산은 금융사고 발생의 우려와 산발적인 관리 체계 및 책임성에 대한 문제가 대두되고 있다. 본 논문에서는 N-스크린 환경 내 금융서비스에 기존 보안위협 및 신규보안 이슈들의 발생에 대해 5가지 관점에서 취약점을 조사 및 분석하고 이에 대한 보안대책을 마련하고자 체계적인 금융 정보보호 프레임워크 개발하였다. 제시한 프레임워크 기반으로 제도관리의 정책체계를 수립하고 기술적 구현방안을 소개함으로써 N-스크린 환경 내 프레임워크의 실 적용성을 고려한 활용방안을 제시한다. 향후 제시한 프레임워크 기반의 응용방안 고도화에 대해 심화 연구할 예정이다.

1) 앱스토어에 등록된 애플리케이션은 등록 전, 검증 센터에서 보안 검사하여 애플리케이션 안전성 여부를 확인

2) 단말관리 프로토콜을 사용하여 모바일 단말의 보안 기능을 원격 제어 및 관리하는 기술로 DM(Device Management) 프로토콜 이용

3) 물리적 보안성 제공하여 외부 공격으로부터 데이터, 키, 인증서 등을 안전하게 보호 및 스마트폰 단말 플랫폼의 무결성 검증을 통해 악성코드 실행을 사전 탐지 및 차단

참 고 문 헌

[1] 현대경제연구원, “스마트 금융의 3대 트렌드와 4대 불안요인”, 경제주평, 444호, pp.1-4, 2011.05.

[2] 홍승필, "N-스크린 정보보호기술", 모바일보안 컨퍼런스, pp5-17, 2011.07.

[3] 배한철, 임양수, 안민지, "커넥트 TV로 인한 미디어 시장 변화 동향 및 시사점", KT 경제경영연구소-IT전략 보고서, 2010.04.

[4] 최철훈, "스마트폰 금융거래 10계명", 금융감독원, 2011.02.

[5] 최재환, "스마트폰 전자금융서비스 안전대책", 보도자료, 금융감독원, 2010.01.

[6] PISA, http://www.nrc-cnrc.gc.ca/eng/ibp/iit/past-projects/software-agent.html

[7] PORTIA, http://crypto.stanford.edu/portia/

[8] ISTPA, http://www.istpa.org/

[9] Safe Harbor Framework, http://export.gov/safeharbor/eu/index.asp

[10] APEC Privacy Framework, http://www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Privacy-Framework.aspx
[11] The Val IT Framework, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Val-IT-Framework-2.0.aspx
[12] IBM's Tivoli, http://www-01.ibm.com/software/tivoli/?pgel=ibmhzn&cm_re=masthead-_-products-_-sw-tivoli
[13] IDMS, http://www.ca.com/us/products/detail/CA-IDMS.aspx
[14] RAPID, http://homepages.laas.fr/deswarte/Publications/RAPID-YDe.pdf
[15] PRIME, http://www.ist-world.org/ProjectDetails.aspx?ProjectId=6a4ab8e175da49528ba38a6d5f52de5e
[16] MIPA, http://portal.acm.org/citation.cfm?id=1766832
[17] APEC Secretariat, "APEC Privacy Framework", 2005 APEC Secretariat, 2005.
[18] 방송통신위원회, 행정안전부, 지식경제부. '2010 국가정보보호백서", 국가정보원, pp.271-273, 2010.04.
[19] 대한민국국회, 법률 제10854호「금융실명거래 및 비밀보장에 관한 법률」, 2011.
[20] 대한민국국회, 법률 제10303호「전자금융거래법」, 2010.
[21] 박세정, "'스마트금융' 보험사까지 확산", 디지털타임스, 2011.06.
[22] 금융보안연구원, "DoS/DDoS 공격 대응 가이드 -SYN Flooding 공격중심-", 2007.10.
[23] 금융보안연구원, "금융부문 암호기술 관리 가이드", 2010.01.
[24] 금융보안연구원, "금융부문 스마트폰 보안 가이드", 2010.12.
[25] 금융보안연구원, "금융부문 IPTV 보안 가이드", 2010.12.
[26] 김소이, "스마트폰과 지급결제 부문의 컨버전스 현황 및 시사점", 금융결제원, 2010.01.
[27] 금융감독원, "금융소비자보호 백서", 2011.04.
[28] 성재모, "전자금융서비스의 환경변화와 보안기술 동향", 금융보안연구원, 2010.12.
[29] 장현미, 김경진, 신유진, 양새로미, 이연우, 김재중, 홍승필. "N-Screen환경 내 금융 프레임워크 개발 방안 연구", 한국인터넷정보학회 추계학술발표대회, 제12권, 제2호, pp.195-196, 2011.
[30] 한국정보통신기술협회, "모바일 서비스", TTA 표준화전략로드맵 보고서, 2011.
[31] Bouguettaya, A.R.A., Eltoweissy, M.Y., "Privacy on the Web: facts, challenges, and solutions", IEEE Computer Society, vol. 1, pp.40-49, 2003.11.
[32] 한국정보통신기술협회, "암호/인증/권한관리", ICT 중점기술 표준화전략맵 Ver.2011, 2011.
[33] 한국정보통신기술협회, "차세대 컴퓨팅", 정보통신 중점기술 표준화로드맵 Ver.2010, 2010.
[34] 김화숙, 이현진, 조기성, "N-Screen 서비스 현황 및 연구 개발 이슈", 정보과학회지, 2011.7, pp. 9-15

◐ 저 자 소 개 ◑

김 경 진

2007년 성신여자대학교 컴퓨터정보학부 졸업 (학사)
2009년 성신여자대학교 대학원 전산학과 (석사)
2009년~현재 성신여자대학교 대학원 컴퓨터학과 (박사과정)
관심분야 : 접근제어, 프라이버시 보호
E-mail : kyongjin@sungshin.ac.kr

서 동 수

1987년 중앙대학교 (학사)
1990년 University of Manchester (석사)
1994년, University of Manchester (박사)
1994~98년 ETRI, 선임연구원
1998년~현재 성신여자대학교 IT학부 교수
관심분야: 정보보호 인증, 소프트웨어 검증
Email : dseo@sungshin.ac.kr

홍 승 필

1993년 Indiana State University (학사)
1994년 Ball State University (석사)
1997년 Illinois Institute of Technology (박사수료)
2002년 (구)한국정보통신대학교 (박사)
1997년~2005년 LG CNS Systems, Inc.
2005년~현재 성신여자대학교 IT학부 조교수
관심분야 : 접근제어, 통합인증, 정보보호 아키텍처, 유비쿼터스 보안, 프라이버시 보호
E-mail : philhong@sungshin.ac.kr