情報保護學會論文誌
第 22 卷 第 2 號, 2012. 4

NFC 환경에서 개인정보보호를 위한 취약점 분석 및 대책 수립 방법론

이 재 식,† 김 형 주,‡ 유 한 나, 박 태 성, 전 문 석
숭실대학교

Analysis on Vulnerability and Establishing Countermeasure Methodologies for Privacy Protection in NFC Environments

Jae-sik Lee,† Hyung-joo Kim,‡ Han-na You, Tae-sung Park, Moon-seog Jun
Soongsil University

요 약

NFC(Near Field Communication)는 근거리 통신 규약으로, 스마트폰 등에 적용되어 그 활용 범위가 매우 넓은 기술이다. 특히, NFC 환경에서 제공되는 서비스는 이용자의 개인정보를 활용한 서비스가 많다. 이러한 서비스에서 이용되는 개인정보는 NFC 기술적 특징 및 스마트폰으로 대표되는 NFC 기기의 특징으로 인해 기존에 없었던 새로운 취약점들이 발생하고 있다. 따라서 본 논문에서는 NFC 환경에서 발생할 수 있는 개인정보와 관련된 취약점을 기술적·관리적·제도적 측면에서 분석하는 방법론 및 그에 따른 대책 수립을 위한 방법론을 제안한다. 또한 제안된 방법론을 통하여 도출된 국내 NFC 서비스의 취약점 및 그에 따른 대책을 제시하고 있다. 본 논문에서 제안된 방법론을 통하여 NFC 환경에서 개인정보보호를 위한 다양한 대책들이 수립될 것으로 기대된다.

ABSTRACT

NFC(Near Field Communication),the short-distance communication protocol, is a technology with a wide range of application applied to smart phones. In particular, many of the services in NFC environments utilize users' privacy information. Privacy information used in such services leads to new vulnerability due to the very features of NFC technology and of NFC devices represented by smart phones. Therefore, the purpose of this study is to suggest a methodology that analyzes privacy vulnerability resulting from a NFC environments in technological, managerial and institutional aspects and a methodology aimed to establish a countermeasure to augment them. Also, this study will suggest vulnerability and countermeasures accordingly in domestic NFC service drawn out through the above methodologies and a countermeasure to improve the vulnerability. It is expected that various safe countermeasures for privacy protection in NFC environments will be established through the suggested methodologies.

Keywords: NFC, Privacy Protection, Analysis on Vulnerability, Establishing Countermeasure, Methodology

접수일(2012년 3월 7일), 게재확정일(2012년 4월 7일)
† 주저자, j30231@ssu.ac.kr
‡ 교신저자, hyungjoo.kim@ssu.ac.kr

I. 서 론

NFC(Near Field Communication)는 13.56-Mhz RF(Radio Frequency) 주파수 영역에서 약 10cm 이하의 짧은 거리로 동작하는 비접촉식 근거리 통신을 위한 기술이다[1]. NFC 기술은 호환성 및 범용성을 위하여 다양한 국제표준 기술을 지원하고 있어[2], 그 활용 범위가 점차 확대되고 있다.

NFC 환경에서 제공되는 서비스는 다양한 개인정보를 활용하는 형태로 전개될 것으로 예상된다. 특히 스마트폰 등을 이용한 NFC 서비스는 위치정보와 같은 사용자에게 민감한 개인정보가 서비스에 포함되어 이용될 수 있다. NFC 기술의 특성상 간단한 터치만으로 서비스가 제공되며, 서비스가 이루어지는 동일 그룹 내에서 사용자의 NFC 서비스 이용패턴이 공유되는 경우, 공유 정보를 이용하여 기존에 수집된 정보 이외의 새로운 사용자 맞춤형 정보를 생성할 수 있다. 이러한 맞춤형 정보는 사용자의 NFC 서비스 이용패턴을 기반으로 생성된 민감한 개인정보이다. 이와 같이 NFC 환경에서는 사용자의 개인정보가 수집·활용되는 다양한 경우가 발생한다.

이에 본 논문에서는 NFC 환경에서 발생할 수 있는 다양한 개인정보보호 취약점을 분석하고 대책을 수립하는 방법론을 제안한다.

본 논문의 구성은 다음과 같다. 1장에서는 본 논문에 대한 소개와 구성을 설명하고, 2장에서는 개인정보의 정의 및 개인정보보호 영향평가와 NFC 기술에 대한 취약점을 살펴본다. 3장에서는 NFC 개인정보보호 방법론을 취약점 분석과 대책 수립의 측면에서 제안하였고, 4장에서는 제안된 방법론을 활용하여 도출된 결과물을 소개하고, 5장에서 결론을 내린다.

II. 관련 연구

본 장에서는 NFC 개인정보보호와 관련하여 개인정보 영향평가 및 NFC 기술적 취약점과 관련된 연구를 살펴본다. 개인정보는 학자나 법률에 따라 다양하게 정의되어 있으나, 본 논문에서는 국내 개인정보보호법의 정의를 사용한다. 개인정보보호법에서 정의된 개인정보란 "살아 있는 개인에 관한 정보로 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)"를 말한다[3]. 즉, 개인과 직접 관련이 없는 정보도 넓은 의미에서 개인정보가 될 수 있다.

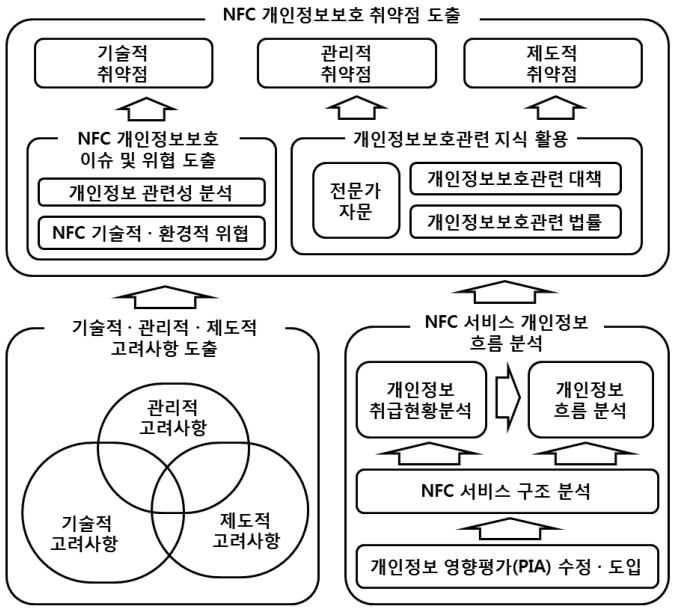
2.1 개인정보 영향평가 (PIA : Privacy Impact Assessment)

개인정보 영향평가란, 개인정보를 활용하는 새로운 정보시스템의 도입이나 개인정보 취급이 수반되는 기존 정보 시스템의 중대한 변경 시 동 시스템의 구축·운영·변경 등이 프라이버시에 미치는 영향(impact)에 대하여 사전에 조사·예측·검토하여 개선 방안을 도출하는 체계적인 절차를 말한다[4]. 개인정보 영향평가는 사전분석 단계, 개인정보 관리현황 분석 단계, 영향평가 결과 정리 단계로 진행된다. 개인정보 관리현황 분석단계는 평가자료 수집 단계, 개인정보 흐름분석 단계, 개인정보침해요인 분석 및 개선방안 도출/위험도산정 단계로 나누어지며, 본 논문에서는 개인정보 흐름분석 단계를 NFC 개인정보보호 취약점 분석 방법론 중 NFC 서비스의 개인정보 흐름도 분석단계에 수정·적용하였다. 개인정보 영향평가의 개인정보 흐름분석은 개인정보 취급 현황분석, 개인정보 흐름표 작성, 개인정보 흐름도 작성, 시스템구조도 작성으로 평가절차가 나누어진다.

2.2 NFC(Near Field Communication) 기술적 취약점

NFC 기술은 13.56Mhz RF 주파수 영역에서 동작하기 때문에 기존의 RFID 환경에서 일어날 수 있는 기술적 취약점과 비슷한 유형의 위협이 발생한다. NFC 기술적 취약점은 도청(Eavesdropping), 데이터 변조(Corruption)·수정(Modification)·삽입(Insertion), 중간자 공격(Man-in-the-Middle-Attack) 등이 있다[5]. 또한 NFC는 NDEF(NFC Data Exchange Format) 메시지 교환 포맷을 이용하여 메시지를 교환할 수 있고, 교환되는 데이터는 RTD(Record Type Definition) 형태로 이루어진다. RTD는 레코드 타입에 따라 다양한 종류가 있으며, NDEF 메시지의 무결성 보장을 위하여 NDEF Signature RTD의 적용이 가능하다. 하지만 NDEF Signature RTD를 적용하여 NDEF를 이용하는 경우도 NFC 기기의 칩셋에 따라 전자서명을 할 수 있는 범위가 달라 무결성이 완벽히 보장된다고 할 수 없다[6].

이러한 NFC 기술적 취약점으로 인해 발생할 수



〔그림 1〕 NFC 개인정보보호 취약점 분석 방법론

있는 문제점은 잠재적인 개인정보를 위협하는 요소이다. 따라서, NFC 기술적 취약점을 해결할 수 있는 방안이 필요하며, 이에 본 논문에서는 NFC 개인정보보호 방법론을 통하여 이를 해결하고자 한다.

III. NFC 환경에서의 개인정보보호를 위한 방법론

NFC 환경에서 개인정보를 보호하기 위해서는, NFC 환경의 개인정보 취약점을 분석하고 그에 따른 대책 수립해서 시행함으로써 개인정보에 안전한 NFC 환경을 구축해야한다. 이에 본 논문에서는 NFC 개인정보보호 취약점 분석 방법론과 NFC 개인정보보호 대책 수립 방법론을 제안한다. 우선 취약점 분석 및 대책 수립은 기술적·관리적·제도적인 3가지 측면에서 접근해야 한다. 이는 단순히 기술적인 문제뿐만 아니라 관리적·제도적 측면으로 인한 문제점도 발생할 수 있기 때문이다. 특히 국가별로 개인정보 관련 법률이 있는 경우, 이는 반드시 지켜야 하는 사항이기 때문에 주의해야 한다.

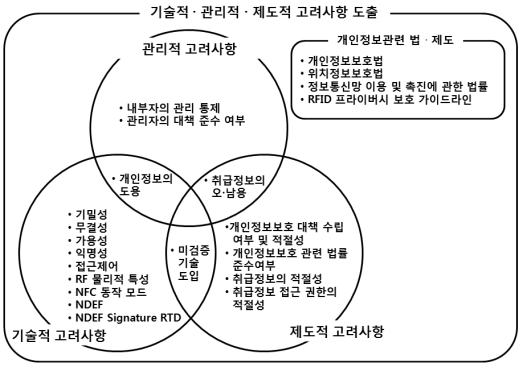
기술적 측면은 NFC 기술의 특성에 따른 부분을 의미하며, 제도적 측면은 법과 같이 반드시 지켜야 하는 측면과 NFC 서비스 업체 등의 자체적인 개인정보보호 정책 수립 등을 의미한다. 관리적 측면은 제도적 측면으로 수립된 정책의 관리가 잘 이루어지고 있는지 등을 의미한다.

3.1 NFC 개인정보보호 취약점 분석 방법론

NFC 환경에서 발생할 수 있는 취약점 분석을 위하여 〔그림 1〕과 같은 NFC 개인정보보호 취약성 분석 방법론을 제안한다. 취약점 분석은 크게 3가지 단계로 구성된다. 첫 번째로 기술적·관리적·제도적 측면에서 고려사항을 도출하는 단계, 두 번째로 NFC 서비스 개인정보 흐름을 분석하는 단계, 마지막으로 이들을 취합하여 NFC 개인정보보호 취약점을 도출하는 단계로 구성된다.

3.1.1 기술적·관리적·제도적 측면 고려사항 도출

기술적·관리적·제도적 측면의 고려사항을 통하여 어떠한 부분에서 개인정보보호 이슈 및 위협이 발생할 수 있는지 분석한다. 〔그림 2〕는 이러한 고려사항 도출 방법을 보여준다. 기술적 고려사항의 예로 일반적인 보안 기술 고려사항인 기밀성, 무결성, 가용성의 정보보안 3대 원칙과 익명성보장 및 접근제어 등을 고려할 수 있다. 또한 NFC 기술·환경적 요인으로 발생할 수 있는 RF 물리적 특성 및 NFC 동작모드, NFC 데이터교환 포맷인 NDEF, NDEF Record



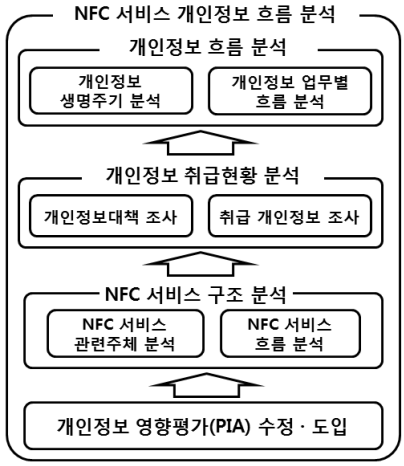
〔그림 2〕 기술적·관리적·제도적 고려사항 도출 방법

의 무결성을 보장하는 NDEF Signature RTD 등을 고려할 수 있다. 제도적 고려사항의 예로 개인정보보호의 대책 수립여부 및 적절성, 개인정보보호 관련 법률의 준수 여부 등이 있다.

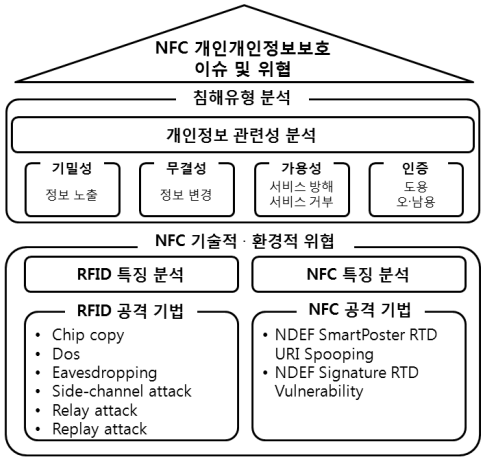
국내의 경우 대표적인 관련 법률로 개인정보보호법, 위치정보보호법, 정보통신망 이용 및 촉진에 관한 법률 등이 있으며 법령은 아니지만 RFID 프라이버시 보호 가이드라인 등도 함께 고려할 수 있다. 또한 취급되는 개인정보의 적절성 및 취급정보별 접근 권한의 설정 등도 제도적 고려사항이 될 수 있다. 관리적 고려사항의 예로 내부자의 관리 통제 및 관리자의 대책 준수 여부 등이 있다. 특정 고려사항은 각 측면에서 공통된 하나 이상의 측면을 가질 수 있다. 개인정보의 도용은 기술적·관리적 고려사항일 수 있으며, 취급정보의 오·남용은 관리적·제도적 고려사항일 수 있다. 또한 검증되지 않은 기술도입은 기술적·관리적 고려사항이 될 수 있다.

3.1.2 NFC 서비스 개인정보 흐름 분석

개인정보 영향평가(PIA: Privacy Impact Assessment)의 개인정보 흐름분석 단계를 수정하여 도입한 NFC 서비스 개인정보 흐름 분석 단계는 〔그림 3〕과 같다. 첫 번째로 개인정보 생명주기에 따른 NFC 서비스 구조를 분석 한다. 이를 위하여 NFC 서비스와 관련된 서비스 주체를 분석하고, 서비스 흐름을 분석한다. 두 번째로 개인정보의 취급현황을 분석한다. NFC 서비스별 개인정보대책이 있는지 조사하고, 각 서비스 주체별 취급하는 개인정보를 분석한다. 마지막으로 개인정보 흐름 분석을 위하여, 개인정보 생명주기에 따른 개인정보 업무별 흐름을 분석하여 NFC 서비스에서 개인정보의 흐름을 분석할 수 있다.



〔그림 3〕 NFC 서비스 개인정보 흐름 분석 방법



〔그림 4〕 NFC 개인정보보호 이슈 및 위협 도출 방법

3.1.3 NFC 개인정보보호 이슈 및 위협 도출

NFC 개인정보보호 이슈 및 위협 도출은 〔그림 4〕와 같이 이루어진다. 첫 번째로 NFC 기술적·환경적 특징을 분석하여 위협을 도출하고, 두 번째로 각 위협별 개인정보와 관련된 침해유형 분석을 통하여 개인정보보호 이슈 및 위협을 도출한다. NFC 기술은 13.56Mhz 영역의 무선주파수를 이용하여 통신하므로 기존의 RFID 환경에서 일어날 수 있는 기술적·환경적 위협과 비슷한 유형의 위협이 발생한다. 따라서 RFID 특징으로 인해 발생할 수 있는 공격 기법과 NFC 특징으로 인해 발생할 수 있는 공격 기법을 도출한다. 도출된 위협은 개인정보와 관련하여 기밀성,

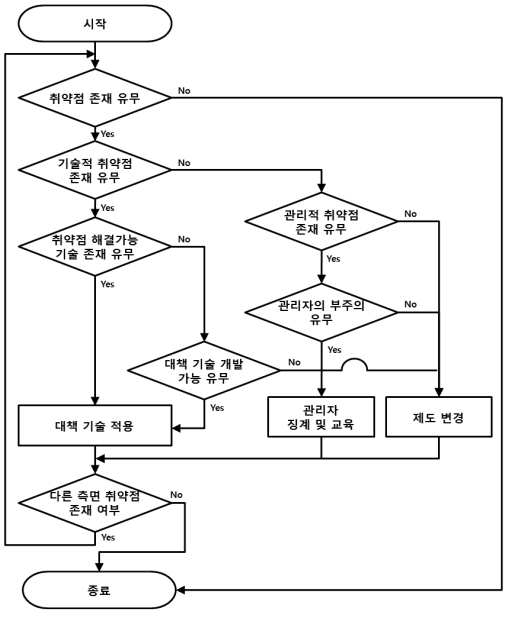
무결성, 가용성, 인증의 4가지 측면에서 개인정보 관련성을 분석한다. 정보의 노출은 기밀성을 침해하며, 정보의 변경은 무결성을 침해한다. 서비스 방해나 거부는 가용성을 침해하며, 도용 및 오·남용은 인증을 침해하는 유형이다.

3.1.4 기술적·관리적·제도적 취약점 도출

NFC 개인정보보호 이슈 및 위협을 고려하고, 기술적·관리적·제도적 측면에서 도출된 고려사항과 분석된 NFC 서비스 개인정보 흐름도를 이용하여 NFC 개인정보보호 취약점을 도출한다. 특히 관리적·제도적 취약점 도출을 위하여 해당분야의 관련 전문가의 자문을 구하거나, 개인정보와 관련된 법률 및 대책 등을 활용하여 보다 객관적인 기술적·관리적·제도적 취약점을 도출할 수 있다. 또한 NFC 서비스별로 마련된 개인정보보호와 관련된 대책도 관리적·제도적 측면에서 검토하여 취약점을 도출 할 수 있다.

3.2 NFC 개인정보보호 대책 수립 방법론

NFC 개인정보보호 취약점 분석을 통하여 도출된 기술적·관리적·제도적 취약점은 〔그림 5〕와 같은 방법을 통하여 모든 측면에서의 대책을 수립한다. 기술적 취약점은 해당 기술을 대체할 수 있는 기술이 있는 경우 이를 활용하고, 그렇지 않은 경우 기술개발을 통하여 취약점을 해결한다. 만약 기술적 취약점을 해결할 수 없는 경우 제도적 변경을 통하여 해당 기술 이외의 다른 기술을 이용하거나 기술적 취약점이 해결될 때까지 잠정적인 서비스 중단 등을 한다. 제도적 취약점이 존재하는 경우 해당 제도의 변경을 통하여 취약점을 해결한다. 관리자의 부주의로 인한 취약점이 발생한 경우 해당 관리자의 징계 및 교육 등을 통하여 취약점을 해결할 수 있으며 그렇지 않은 경우 제도의 변경을 통하여 관련 취약점을 해결한다. 취약점 해결 후 다른 측면의 취약점이 존재하는 경우 다시 처음으로 돌아가서 취약점을 해결한다.



〔그림 5〕 NFC 개인정보보호 대책 수립 방법론

IV. NFC 개인정보보호 방법론 활용방안

본 장에서는 본 논문에서 제안한 NFC 개인정보보호 방법론을 활용하여 분석된 NFC 개인정보보호 취약점 및 대책 예시를 설명한다〔7〕. 분석된 NFC 개인정보보호 취약점과 대책을 활용하여 NFC 개인정보보호 가이드라인 및 수칙 등과 같은 내용을 도출하였고, 이를 활용하여 NFC 서비스 사업자가 NFC 환경에서 개인정보에 안전한 NFC 서비스를 제공할 수 있을 것으로 기대한다. 이와 관련된 자세한 내용은 참고문헌〔7〕을 참조하기 바란다.

4.1 NFC 개인정보보호 취약점 분석 예시

본 논문에서 제안한 NFC 개인정보보호 취약점 분석 방법론을 통하여 도출된 취약점은 〔표 1〕과 같다. 각 취약점은 기술적·관리적·제도적 고려사항 및 NFC 서비스 개인정보 흐름도 분석을 통하여 도출되었으며, 도출에 사용된 NFC 서비스는 국내에서 제공되고 있는 서비스인 결제, 마일리지, 쿠폰, 스탬프, 예매 서비스이다. 또한 〔그림 4〕의 개인정보보호 이슈 및 위협 도출 방법을 통하여 도출된 취약점도 기술적 취약점에 포함하였다.

4.2 NFC 개인정보보호 대책 수립 예시

본 논문에서 제안한 NFC 개인정보보호 대책 수립 방법론을 통하여 〔표 1〕에서 도출된 취약점에 관한 대책은 〔표 2〕와 같다. 제시된 대책은 개인정보보호 대책 수립 적절성 및 개인정보보호 관련 법률 준수 여부

〔표 1〕 국내 NFC 서비스 취약점 분석표 예시

구분	취약점	설명
기술적	도청의 위협	전송되는 데이터를 도청 할 수 있음
	데이터 변조	전송되는 데이터를 변조 할 수 있음
	데이터 수정	전송되는 데이터를 수정 할 수 있음
	데이터 삽입	전송되는 데이터에 추가적인 데이터를 삽입 할 수 있음
	중계 공격	악의적인 사용자가 중간에서 데이터를 가로채어 중계 공격을 할 수 있음
	중간자 공격	악의적인 사용자가 중간에서 데이터를 가로채어 중간자 공격을 할 수 있음
	스마트 포스터 URI 스푸핑	URI 주소를 스푸핑 할 수 있음
	NDEF Signature RTD 취약점	NDEF 메시지가 위조되었으나 서명은 유효한 경우가 발생할 수 있음
	개인정보 암호화 부분적 미지원	저장되는 개인정보를 암호화 하지 않아 개인정보 노출 시 기밀성에 문제가 있음
	모바일 APP 종료상태에서 모바일 신용카드 결제 가능	사용자의 인지 과정 없이 결제가 가능한 문제가 있음
관리적	내부 개인정보 유출 사고	악의적 내부자로 인한 개인정보 유출 사고가 발생할 수 있음
관리적/제도적	불필요한 개인정보 수집 및 저장	필요 이외의 개인정보를 수집하고 저장할 수 있음
	서비스 이용시 추가 개인정보 요구	서비스 이용 시점에서 추가적 개인정보를 요구할 수 있음
	서비스 이용 지점 정보 수집 및 저장	사용자의 서비스 이용 패턴이 분석될 수 있음
제도적	모바일 APP에서 자사 웹 사이트 자동 로그인 기능 지원	모바일기기의 분실 등으로 인한 불법 사용 시 인증된 사용자인지 확인 불가능
	모바일 APP에서 모바일 신용카드 정보 확인 가능	신용카드의 오·남용이 발생할 수 있음
	모바일 APP에서 과다 개인정보 저장	과다 개인정보의 저장은 잠재적 보안위협요소임
	개인정보의 과도한 제공 및 위탁	과도한 개인정보의 제공 및 위탁은 잠재적 보안위협요소임
	개인정보 활용 동의에 따른 정보 무단 활용(스팸)	스팸 광고를 유발할 수 있음
	개인정보 파기 약관 비존재	사용자는 개인정보의 파기 절차를 알 수 없음
	개인정보 위탁 처리 및 정보업체 명시 불이행	사용자가 원하지 않는 업체에서의 위탁이 일어날 수 있음
	결제 시 신용카드 번호 출력방식에 따른 카드번호 노출 위험	신용카드의 오·남용이 발생할 수 있음

가 고려되었으며, 실제로 일부 대책의 경우 분석된 NFC 서비스에 반영되어 관련된 취약점이 해결되었다.

V. 결 론

NFC 환경에서 개인정보를 보호하기 위하여, 본 논문에서는 개인정보보호 취약점 분석 및 그에 대한 대책을 수립 위한 방법론을 제안하였다. NFC 환경에서 발생할 수 있는 개인정보와 관련된 취약성은 기술적인 측면뿐만 아니라, 관리적·제도적 측면에서도 이루어져야 한다. 특히, 국내의 경우 개인정보보호법의 시행과 함께 법·제도적인 측면에서 개인정보의 관리는 매우 엄격하고 안전하게 다루어져야 할 것이다. 따라서 본 논문에서는 개인정보보호 관련 법·제도 등을 고려하여 NFC 환경에서 안전하게 개인정보가 활용될 수 있도록 방법론을 제안하였다. 4장의 NFC 개인정보보호 방법론 활용방안에서 살펴본 NFC 개인정보보호 취약점 및 대책은 국내에서 서비스 되고 있는 일부 서비스를 대상으로 도출된 취약점 및 대책의 예시이다. 따라서 예시에 포함되지 않은 NFC 서비스는 도출된 취약점 이외의 다른 취약점이 존재할 수 있으나, 제안된 방법론을 통하여 쉽게 새로운 취약점을 발견하고 그에 대한 대책을 마련할 수 있을 것으로 기대한다.

〔표 2〕 국내 NFC 서비스 취약점에 따른 대책 예시

구분	취약점	대책
기술적	도청의 위협	보안채널을 이용하여 도청된 데이터에 기밀성을 부여
	데이터 변조	RF 필드 체크를 통한 데이터 변조·수정·삽입 확인 가능하며, 보안채널 이용 시 변조·수정·삽입된 데이터는 의미 없는 데이터임
	데이터 수정	
	데이터 삽입	
	중계 공격	타이밍 체크와 위치 체크를 통하여 중계공격을 예방가능
	중간자 공격	RF 필드 체크로 중간자공격이 일어나는지 확인 가능하며, 사전비밀 공유를 통한 통신 시 중간자 공격은 실패
	스마트 포스터 URI 스푸핑	URI 검증 및 URI 문법 체크
	NDEF Signature RTD 취약점	NDEF Record의 헤더필드에 대한 전자서명 지원
	개인정보 암호화 부분적 미지원	비밀번호 및 바이오정보는 일방향 암호화 사용하고, 그 외 개인정보는 안전한 암호화알고리즘 사용
	모바일 APP 종료상태에서 모바일 신용카드 결제 가능	NFC 기능 On/OFF 설정 지원하고, 모바일 APP에 PIN 설정 지원
관리적	내부 개인정보 유출 사고	직원에 대해 개인정보보호법규 및 개인정보와 정보시스템의 안전관리에 관한 직원의 역할 및 책임에 대해 교육 실시 및 직원 채용 및 위탁계약서에 직무상 취급한 개인정보의 누설 금지 의무를 명시하고 제재조치 마련
관리적/제도적	불필요한 개인정보 수집 및 저장	불필요한 개인정보의 수집 및 저장을 막기 위해 개인정보의 수집 목적을 설정하고 수집되는 개인정보에 대해 책임을 마련
	서비스 이용 시 추가 개인정보 요구	개인정보책임자에게 서비스 이용 시 추가적으로 발생하는 개인정보에 대해서 이용자에게 알리고 동의를 받는 절차를 수립
	서비스 이용 지점 정보 수집 및 저장	서비스 이용 지점의 직원에 대한 개인정보 교육을 실시하고 안전한 개인정보 저장을 위해 보호조치에 대한 내부계획을 수립
제도적	모바일 APP에서 자사 웹 사이트 자동 로그인 기능 지원	4자리 이상의 PIN을 입력하도록 로그인 기능 설정
	모바일 APP에서 모바일 신용카드 정보 확인 가능	모바일 신용카드 정보를 확인 할 경우 로그인 및 PW 기능 설정하고, 그렇지 않는 경우 공개되어도 될 정보나 부분 암호화하여 확인하도록 설정
	모바일 APP에서 과다 개인정보 저장	NFC 단말기 모바일 APP에 최소한의 개인정보만을 저장하고, 암호화하여 저장
	개인정보의 과도한 제공 및 위탁	이용자에게 제 3자 제공 및 업무 위탁의 내용을 명시하고 동의를 얻을 수 있도록 함
	개인정보 활용 동의에 따른 정보 무단 활용(스팸)	이용자에게 개인정보의 이용 목적 및 제공에 대해 알리고 E-mail 및 SMS에 대한 정보 제공을 거부할 수 있도록 설정
	개인정보 파기 약관 비존재	이용자에게 개인정보의 이용 목적 달성 및 보유기간 경과 시 개인정보를 파기한다는 약관 설정
	개인정보 위탁 처리 및 정보업체 명시 불이행	개인정보를 취급하여 업무 위탁의 경우 이용자에게 알리고 동의를 얻음
	결제 시 신용카드 번호 출력방식에 따른 카드번호 노출 위험	신용카드 번호와 같은 결제 관련 개인정보는 암호화하여 저장 및 전송
	불필요한 개인정보 수집 및 저장	제도의 변경으로 반드시 필요한 정보만을 수집
	서비스 이용 시 추가 개인정보 요구	추가 개인정보의 수집 목적을 이용자에게 명시하고 동의를 얻음
	서비스 이용 지점 정보 수집 및 저장	이용자의 서비스 이용에 대한 정보를 수집 및 저장에 관한 이용자의 동의를 얻음

참고문헌

〔1〕 ISO/IEC, "ISO/IEC 18092, Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1)", 2004.

〔2〕 ISO/IEC, "ISO/IEC 21481, Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol-2 (NFCIP-2)", 2005.

〔3〕 법제처, 개인정보보호법, 2011.

〔4〕 행정안전부, 한국인터넷진흥원, 공공기관 개인정보 영향평가 수행 안내서(개정판), 2011.

〔5〕 Ernst Haselsteiner, Klemens Breitfuß, "Security in Near Field Communication(NFC)", Workshop on RFID Security RFIDsec, 2006.

〔6〕 Michael Roland, Josef Langer, Josef Scharinger, "Security Vulnerabilities of the NDEF Signature Record Type", Workshop on Near Field Communication, 2011.

〔7〕 숭실대학교 산학협력단, NFC 개인정보보호 대책 연구, 한국인터넷진흥원, 2012.

〈著者紹介〉

이 재 식 (Jae-sik Lee) 학생회원
2005년 8월: 경원대학교 컴퓨터공학과 졸업
2007년 8월: 숭실대학교 컴퓨터학과 석사
2007년 9월~현재: 숭실대학교 컴퓨터학과 박사과정
〈관심분야〉 RFID, NFC, 개인정보보호, 인증이론 및 시스템, 암호프로토콜

김 형 주 (Hyungjoo Kim) 학생회원
2008년 8월: 단국대학교 컴퓨터과학과 졸업
2010년 8월: 숭실대학교 컴퓨터학과 석사
2010년 9월~현재: 숭실대학교 컴퓨터학과 박사과정
〈관심분야〉 RFID, NFC, 개인정보보호, 인증, 암호프로토콜, 전자정부

유 한 나(Han-na You) 학생회원
2008년 8월: 평생교육원 정보보안전공 공학사
2010년 8월: 숭실대학교 컴퓨터학과 공학석사
2010년 9월~현재: 숭실대학교 컴퓨터학과 박사과정
〈관심분야〉 금융보안, 인증, 네트워크보안, 개인정보보호

박 태 성 (Tae-Sung Park) 학생회원
2011년 8월: 숭실대학교 컴퓨터학과 석사
2011년 9월~현재: 숭실대학교 컴퓨터학과 박사과정
〈관심분야〉 정보보호, 네트워크 보안, 인증, PKI

전 문 석 (Moon-seog Jun) 정회원
1981년 2월: 숭실대학교 전자계산학과 졸업
1986년 2월: University of Maryland Computer Science 석사
1989년 2월: University of Maryland Computer Science 박사
1986년 9월~1989 12월: University of Maryland 강사
1989년 3월~7월: Morgan State University 조교수
1989년 9월~1991년 2월: New Mexico State University Physical Science Lab. 책임연구원
1991년 3월~현재: 숭실대학교 정교수
〈관심분야〉 정보보호, 네트워크 보안, 전자여권, 암호학