NFC 프로그램 메시지 방식에서 변조 방지와 사용자에 의한 동적 접근 제어 방법

(A Method of Forgery Protection and User's Dynamic Access Control in NFC Program Messages)

고 명 필 † 최 광 훈 †† 임 효 상 ††
(Myungpil Ko) (Kwanghoon Choi) (Hyo-Sang Lim)

요 약 표준 NFC 메시지와 호환되는 프로그램 메시지 방식에서 메시지 변조 방지와 사용자에 의한 동적 접근 제어 방법으로 NFC 서비스 보안을 높이는 방법을 제안한다. 이 방법을 안드로이드 모바일 환경에서 구현하고 실험한 결과 상용 NFC 태그 용량의 크기 이내에서 프로그램 메시지를 작성할 수 있고 두 가지 보안 방법을 고려한 NFC 서비스 시간도 사용자 입장에서 기존 NFC 메시지 방식과 큰 차이가 없음을 확인하였다.

키워드: NFC, 보안, 인증서, 접근제어, 안드로이드 플랫폼

Abstract This paper proposes a method of forgery protection and user's dynamic access control in NFC standards compliant program messages. We implement this proposal in Android phones to test mobile applicability. The sizes of benchmark program messages are small enough to be stored in stock NFC tags, and the total execution time increased due to employing the two security methods is not noticeable to users in NFC service.

Keywords: NFC, security, certificate, access control, android platform

1. 서 론

NFC(Near Field Communication)[1]은 13.56MHz 주파수 대역을 이용하는 비접촉식 근거리 통신 기술이다. NFC를 지원하는 모바일 폰과 NFC 태그를 서로 10cm 이내 거리에 두면 태그에 기록된 정보가 모바일 폰에 전송되는 기술이다.

NFC 포럼에서는 태그에 저장되는 정보(NFC 메시지)의 표준 형식 NDEF(NFC Data Exchange Format)을 정의하였다[2]. 자바(Java, JSR-257)[3]와 안드로이드 플랫폼에서 제공하는 NFC API[4]는 모두 NDEF를 지원한다.

NDEF로 작성된 NFC 메시지(NDEF 메시지) 외에 [5]에서 프로그램 메시지 방식을 처음으로 제안하였다. 표준 NDEF 메시지에서 NFC 서비스 식별자의 범위가 URI[6], 텍스트[7], 스마트 포스터[8]로 제한되어 호환성 문제가 있다. 즉, 표준 범위 외의 NFC 서비스를 제공하기 위해 서비스 제공자가 임의로 식별자를 정의하면 다른 서비스 제공자가 알지 못하는 호환성 문제가 있다. 프로그램 메시지 방식은 태그에 NFC 서비스의 식별자를 저장하는 대신 NFC 서비스를 제공하는 프로그램 자체를 저장하여 식별자 호환성 문제를 해결하였다.

그러나 NFC 메시지로 NDEF 메시지와 프로그램 메시지 방식 중 어느 것을 선택하더라도 NFC 메시지 변조 문제와 NFC 메시지로 인해 수행되는 액션이 모바일 폰의 중요 정보를 삭제 또는 유출하는 보안 문제가 발생할 수 있다. 이러한 두 가지 NFC 보안 문제를 해결

· 본 논문은 2013년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2011-0009225)

† 학생회원 : 연세대학교 컴퓨터정보통신공학부
myungpil.ko@yonsei.ac.kr
†† 정 회 원 : 연세대학교 컴퓨터정보통신공학부 교수
(Yonsei Univ.)
kwanghoon.choi@yonsei.ac.kr
(Corresponding author임)
hyosang@yonsei.ac.kr

논문접수 : 2013년 9월 12일
심사완료 : 2013년 10월 20일

표 1 기존 연구와 비교
Table 1 Comparison with Related Work

	Message Type	NDEF Format Compatible	Forgery Check	Access Control
NDEF	Identifiers	O	X	X
[5]	Program	X	X	Admin
This Paper	Program	O	O	User

한 연구가 없었다. 이 논문은 프로그램 메시지를 사용하는 NFC 서비스에서 이 문제를 해결하여 보안을 강화하는 방법을 제시하고 높은 보안성과 함께 NFC 서비스의 모바일 사용성도 기존 NDEF 메시지 방식의 수준으로 보장함을 실험을 통해 보인다.

본 논문에서 기여한 점은 첫째, NDEF와 호환되는 프로그램 메시지 방식을 제안하고, 둘째, 인증서를 사용하여 프로그램 메시지의 변조를 방지하는 방법을 제안하고, 셋째, 프로그램 메시지를 통한 NFC 서비스의 상세 내용을 사용자가 직접 제어하는 방법을 제안한다. 넷째, 기존 NDEF 메시지 방식의 수준과 동일한 NFC 서비스 사용성을 보장함을 실험으로 보인다.

NDEF 표준과 기존 연구[5]와 이 논문에서 수행한 연구 내용과의 비교는 표 1과 같이 요약될 수 있다.

본 논문의 구성은 다음과 같다. 2장에서 관련 연구를 기술하고, 3장에서는 NDEF 형식[2]으로 프로그램 메시지[5]를 표현하는 방법을 제안한다. 4장에서는 보안 방법 두 가지를 제안하고, 5장에서 실험결과를 설명한 다음, 6장에서 결론을 맺고 향후 연구를 논의한다.

2. 관련 연구

2.1 NDEF 메시지 방식

NFC 포럼에서 정의한 NDEF 메시지는 한 개 이상의 NDEF 레코드를 포함하는 형태이다. NDEF 레코드의 형식을 정의하는 표준 타입으로, URI 레코드 타입[6]과 텍스트 레코드 타입[7]은 각각 URI와 텍스트를 표현하는 방법을 제공하고, 스마트 포스터 레코드 타입[8]은 간단한 프로그래밍 방법을 제공하는데 “실행”, “나중을 위해 저장”, “수정을 위해 열기”와 같은 포괄적인 의미의 (서비스 제공자가 그 의미를 정하는) 3가지 명령어가 표준으로 정의되어 있다. 제네릭 컨트롤 레코드 타입[9]은 보다 더 일반적인 명령어를 표현하는 방법을 제공하지만, 명령어 어휘는 표준의 범위에 포함되지 않아서 서비스 제공자들은 비 호환 명령어들을 사용한다.

표 2에서 표준 NDEF 레코드 타입의 종류와 각 타입에 대한 예를 보여준다. 표에서 보여주는 NDEF 레코드, 예를 들어 전화번호를 표현하는 NDEF 메시지 “*U tel:+35891234567*”은 그림 1과 같이 구성되어 있다. TYPE

표 2 NDEF 레코드 타입
Table 2 NDEF Record Type

Text	T Hello World
URI	U tel:+35891234567
Smart Poster	Sp, U http://www.nfc-forum.org, act Launch browser, T Hello World
Generic Control	Gc, Target: Propery Manager, Action: Set, Data: Silent Mode ON

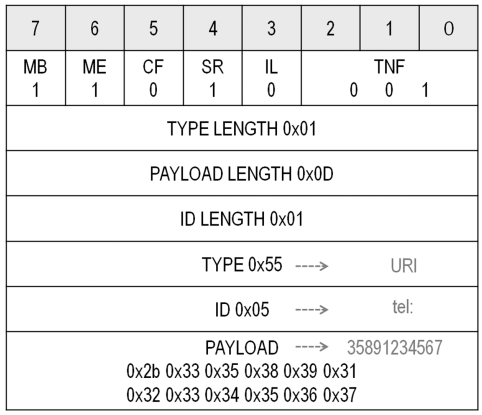

그림 1 NDEF URI 레코드
Fig. 1 NDEF URI Record

필드의 “*U*”는 URI를, ID 필드의 “*tel:*”은 주소 프로토콜을, PAYLOAD 필드는 전화번호를 나타낸다.

NDEF 메시지의 식별자는 각 레코드 타입의 구분 문자열 “*T*”, “*U*”, “*Sp*”, “*Gc*”와 각 타입에서 사용하는 세부 명령어 어휘를 조합하여 구성된다. 세부 명령어 어휘란, URI 레코드 타입의 경우 주소 프로토콜 “*tel:*”, 스마트 포스터 레코드 타입의 경우 “*act Launch browser*”, 제네릭 컨트롤 레코드 타입의 경우 “*Action Set*” 등을 가리킨다.

NDEF 메시지 방식에서는 이러한 NDEF 메시지 식별자를 서비스 제공자가 부여하는 의미로 해석하여 NFC 서비스를 제공한다. 즉, 각 식별자와 해당 NFC 서비스를 제공하는 코드를 연결하는 일종의 매핑 테이블을 통해 구현한다.

NDEF 메시지 방식은 식별자 호환성 문제가 있다. 예를 들어 벨소리를 무음으로 바꾸는 표준에 없는 NFC 서비스를 제공하기 위해 이 서비스에 대한 식별자를 임의로 정하면 다른 서비스 제공자는 처리하지 못한다. 또한, 표준 식별자에 대해서도 해당하는 서비스의 엄밀한 의미를 정의하지 않아 서비스 제공자의 해석에 의존한다. 식별자 호환성 문제에 대응하기 위해 [5]에서는 프로그램 메시지 방식을 처음 제안하였다.

이 외에도 NDEF 메시지 방식은 보안에 취약한 문제

가 있다. 태그 변조에 대응하는 방법이 없으며, 특정 식별자로 인해 수행되는 서비스가 사용자에게 유해한 내용인 경우라도 사용자가 이를 수행하지 않도록 제어하는 방법이 없다.

2.2 프로그램 메시지 방식

NDEF 메시지 방식에서 식별자 호환성 문제를 해결하기 위해 [5]에서 처음으로 프로그램 메시지 방식을 제안하였다. NFC 메시지에 NFC 서비스의 식별자를 저장하는 대신 NFC 서비스를 제공하는 프로그램을 저장하는 방식이다. 스킴(Scheme) 프로그래밍언어[10]를 선택해 사용하고 안드로이드 플랫폼 API를 조합해서 NFC 서비스를 제공하는 프로그램을 작성한다[5].

NDEF 메시지 "*U tel:+35891234567*"에 해당하는 프로그램 메시지에 저장된 스킴 프로그램은 다음과 같다.

```
(define number
  (android.net.Uri.parse "tel:35891234567"))
(define dial (android.content.Intent.
  (android.content.Intent.ACTION_CALL$) number)
(.startActivity context dial)
```

스킴 해석기를 통해 프로그램 메시지에 저장된 프로그램을 실행하면서 NFC 서비스에 필요한 안드로이드 플랫폼 API를 호출한다. 위의 예제에서는 안드로이드 플랫폼의 전화 걸기 API를 사용하였다.

스킴 프로그래밍언어와 안드로이드 플랫폼 API 집합은 명확히 정의되어 있으므로 이를 표준으로 정함으로써 NDEF 메시지 방식의 식별자 호환성 문제를 해결할 수 있다.

프로그램 메시지 방식에서는 프로그램이 사용할 수 있는 API 범위를 관리자가 지정해 NFC 서비스 사용자의 중요 정보를 삭제하거나 유출되는 문제에 대응하였다[5]. 안드로이드 플랫폼 API 집합을 사용할 수 있는 샌드박스(sandbox)에서 스킴 프로그램을 실행하도록 해석기를 구성하였다.

하지만 프로그램 메시지 변조에 대한 대응을 고려하지 않았고, 허용 가능한 API가 제한적이어서 다양한 NFC 서비스 구현이 어렵다. 또한, 프로그램 메시지 방식은 NDEF와 호환성을 고려하지 않은 단점도 있다.

2.3 NFC 보안에 대한 기타 관련 연구

이 외에도 NFC 보안에 대한 기존 연구들[11-13]이 있지만 NFC 물리 계층이나 링크 계층에서 태그 변조, 중간자 공격(Man-in-the-Middle Attack), 릴레이 공격(Realy Attack)과 그 대응 방법에 대한 것이다. 본 논문은 NFC 응용 계층에서의 NFC 메시지 변조 및 서비스에서 보안 문제를 다루고 있다. 이들 연구 결과를 본 논문의 연구 결과와 함께 활용하면 여러 계층에서 NFC 보안을 강화할 수 있을 것이다.

3. NDEF와 호환되는 프로그램 메시지 형식

먼저 프로그램 메시지를 MIME 타입의 NDEF로 표현하는 방법을 제안한다. 이 NDEF 기반 프로그램 메시지에서는 TNF(Type Name Format) 필드를 0x02(MIME 타입)으로 지정하고 TYPE 필드에 아래의 타입을 지정한다.

- mime/scheme : NDEF 레코드의 PAYLOAD 필드에 스킴 코드를 직접 저장한다.
- mime/schemeZip : NDEF 레코드의 PAYLOAD 필드에 ZIP으로 압축된 스킴 코드를 저장한다.
- mime/schemeUrl : 스킴 코드가 저장된 서버의 URL을 NDEF 레코드의 PAYLOAD 필드에 저장하고, 네트워크를 통해 코드를 내려받는다.
- mime/schemeEncrypted : 프로그램 메시지는 세 개의 레코드로 구성된다. 첫 번째 레코드에 스킴 코드를, 두 번째 레코드에 작성자의 인증서로 암호화한 프로그램 해시 값을, 세 번째 레코드에 프로그램 작성자의 인증서를 각각 저장한다.

그림 2는 본 논문에서 제안한 mime/scheme 타입을 사용한 NDEF 기반 프로그램 메시지다.

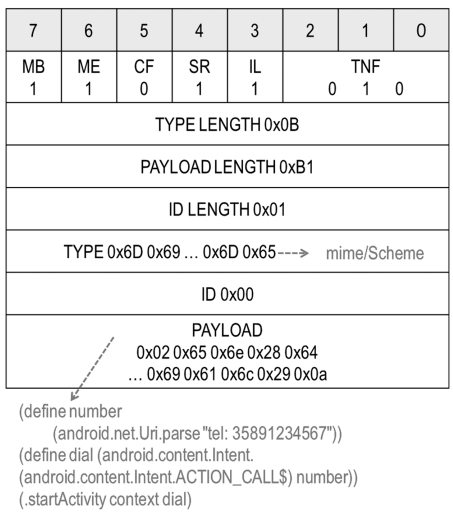

그림 2 NDEF 기반 프로그램 메시지
Fig. 2 A Program Message in NDEF

4. NFC 서비스 보안 방법

4.1 인증서 기반 프로그램 메시지 변조 방지

프로그램 메시지를 악의적으로 변조하는 문제에 대응

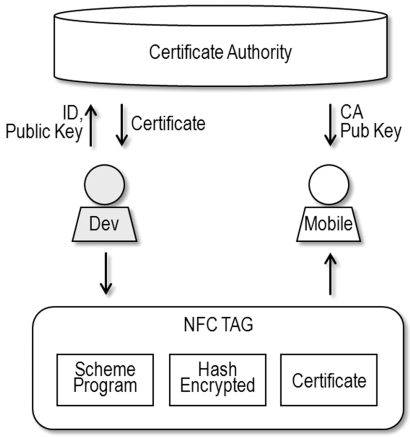

그림 3 NFC 서비스에서 인증서 관리
Fig. 3 Certificate Management in NFC Service

하기 위해 그림 3과 같이 인증서 기반 변조 검사 방법을 제안한다. 이 방법은 다음의 여섯 단계로 구성한다.

첫째, 개발자는 인증기관에 아이디와 공개키를 등록하고, 인증기관은 비밀키로 개발자의 아이디와 공개키를 암호화하여 인증서를 만들어 개발자에게 돌려준다. 둘째, NFC 태그에 프로그램 메시지를 저장할 때 암호화된 해시 값과 인증서를 추가로 저장한다. 셋째, 사용자는 NFC 플랫폼 설치 시 인증기관의 공개키를 받는다. 넷째, NFC 태그에 저장된 프로그램, 해시 값, 인증서를 내려받는다. 다섯째, 인증기관의 공개키로 개발자의 인증서를 복호화하여 개발자의 아이디와 공개키를 얻어 이를 이용하여 암호화된 해시 값을 복호화한다. 여섯째, 프로그램 실행 전 아이디를 확인하고 프로그램의 해시 값을 계산해 복호화한 해시 값을 비교하여 코드 변조를 확인한다.

악의적인 목적으로 프로그램 메시지를 변경했을 경우 전달받은 암호화된 해시 값을 인증서로 복호화한 것과 저장된 프로그램으로부터 구한 해시 값을 비교하면 서로 일치하지 않게 되어 코드 변조를 확인할 수 있다.

4.2 사용자의 동적 접근제어 방법

프로그램 메시지로 인해 수행되는 액션이 사용자의 중요 정보를 삭제하거나 유출하는 보안 문제에 대응하고자 사용자가 NFC 서비스 진행에 직접 개입하는 동적 접근제어 방법을 제안한다. [5]에서는 관리자가 안전하다고 판단되는 API 집합만을 지정하여 허가하는 방식을 사용하는데 이 경우 다양한 NFC 서비스를 구현할 때 필요한 API를 사용 못하는 문제가 발생할 수 있다.

사용자의 동적 접근제어 방법은 다음과 같다. 처음에는 모든 안드로이드 API에 대해 사용자 허가를 받아야 하는 설정으로 초기화한다. NFC로 내려받은 스킴 프로그램이 안드로이드 플랫폼 API를 사용할 때마다 사용자로 하여금 API 명을 확인하고 실행 여부를 결정하게 한다. API 사용을 요청한 시점에 한 번 허가하는 옵션과 이후에 동일 API 사용을 요청하면 모두 허가하는 옵션을 사용자가 선택할 수 있다.

제안한 방법은 개발자 입장에서 다양한 API를 사용하여 프로그램 메시지를 작성할 수 있게 하고 사용자 입장에서 직접 API 접근을 제어할 수 있어 보안 문제에 유연하게 대응할 수 있는 장점이 있다.

그럼에도 불구하고 사용자가 API 상세 내용에 대해 알지 못하여 API 사용을 무조건 허가하는 부작용이 발생할 수 있다. 이 문제를 해결하기 위해 본 논문에서 제안한 사용자의 동적 접근제어 방법과 [5]에서 제안한 관리자 주도의 동적 접근제어 방법을 혼합하여 사용자의 결정을 최소화할 수 있다. 다른 해결 방법으로 PCC(Proof Carrying Code)[14] 아이디어를 사용하는 정적 접근제어 방법이 있다. 프로그램 메시지에 스킴 프로그램의 보안 분석 결과도 함께 NFC 태그에 저장해 전달하고 모바일 디바이스에서 스킴 프로그램과 보안 분석 결과를 비교해 보안 사항을 확인한 다음 실행하는 방법이다.

5. 구현 및 논의사항

5.1 구현

앞에서 제안한 두 가지 보안 방법을 사용한 안전한 NFC 플랫폼의 아키텍처는 그림 4와 같다.

이 아키텍처에서 가정하는 시나리오는 다음과 같다. 사용자가 NFC 태그로부터 인증서 기반 프로그램 메시지를 모바일 폰에 내려받는다. 공개키 기반 변조 검사를 수행하여 변조되지 않은 경우에만 스킴 프로그램을 실행한다. 스킴 해석기(Scheme Interpreter)에서 스킴 프로그램을 해석하고 필요에 따라 안드로이드 API를 실행한다. 이때 이 API를 실행해도 되는지를 사용자에게 묻

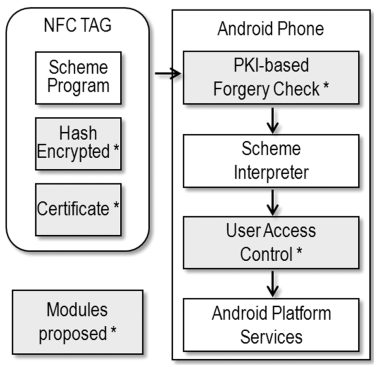

그림 4 안전한 NFC 플랫폼 아키텍처
Fig. 4 A Secure NFC Platform Architecture

고 허가 여부에 따라 진행한다.

제안한 아키텍처를 안드로이드 환경에서 구현하였고, 구현 소스와 실험에 사용한 스킴 프로그램 예제는 다음 사이트에서 확인할 수 있다.

- 소스: https://github.com/nzzzn/safeNFCTaskApp
- 예제: http://mobilesw.yonsei.ac.kr/nfc/jscheme/

5.2 모바일 환경에서 제안한 방법의 적용성 실험

제안한 안전한 NFC 플랫폼 아키텍처를 통해 보안성을 높이는 것도 중요하지만 실제 모바일 폰 환경에서의 활용성을 확인하는 것도 중요하다. 그림 5와 같이 안드로이드 기반 넥서스 S 모바일 폰과 상용 NFC 태그를 이용하여 구현 및 실험하였다.

실험에서는 표 3에서와 같이 프로그램 메시지의 크기와 상용 태그의 용량을 비교하고, 인증서 기반 변조 검사 과정으로 인한 시간 오버헤드를 측정하였다.

제안한 방법으로 프로그램 메시지를 작성하면 암호화된 해시 값과 인증서가 추가되어 약 800바이트가 증가했다. 예제로 사용한 프로그램 메시지의 전체 크기는 1~1.3K바이트이다. 현재 상용 NFC 태그의 용량은 1~8K바이트이다. 압축 형식을 사용하면 최소 용량의 NFC 태그에도 저장 가능하다.

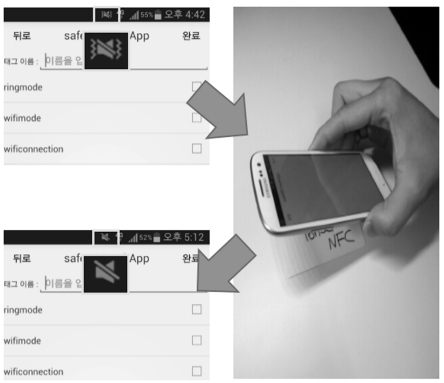

그림 5 NFC를 이용한 벨소리 설정 토글

Fig. 5 A Scenario of Ring Tone Toggle in NFC

표 3 실험 결과

Table 3 An Experimental Result

Program	Program Size	Program +Certificate+ Hash Size	Forgery Check + Run-Time	Forgery Check Time
Ring Mode	512B	1339B	150ms	2ms
WIFI On/Off	233B	1060B	140ms	10ms
WIFI Connection	408B	1235B	155ms	5ms
App Start	203B	1030B	170ms	6ms
Ring Volume	226B	1053B	179ms	13ms

변조 검사에 걸리는 시간은 2~13ms가 소요되었다. 변조 검사와 동적 제어를 적용한 상황에서 전체 프로그램 실행 시간은 140~179ms로 확인하였다. NDEF 메시지 방식의 처리시간은, 예를 들어 URI 레코드를 읽고 웹 브라우저를 호출하기까지의 시간은 대략 10ms이다. 두 방식 모두 0.2초 이내에 NFC 서비스가 완료되어 모바일 사용자 입장에서 느낄만한 시간 차이는 아니다.

6. 결론 및 향후연구

프로그램 메시지 방식의 NFC 서비스에서 메시지 변조 방지와 사용자의 서비스 동적 제어 방법을 제안하였고, 실험을 통해 제안한 방법이 안드로이드 모바일 환경에서 적용 가능함을 보였다.

향후 연구 주제로 스킴 구문과 안드로이드 API를 혼합해 프로그래밍할 때 발생하는 오류를 타입 검사를 통해 사전에 검사하는 방법에 대한 연구가 있다.

References

[1] Roy Want, "Near Field Communication," *IEEE Pervasive Computing*, vol.10, no.3, pp4-7, Jul. 2011.

[2] NFC Forum. (2006, Jul 24). NFC data exchange format (NDEF) technical specification [Online]. Available: http://www.nfc-forum.org/home/ (downloaded 2013, Sep. 10)

[3] Java NFC API. (2013). JSR257 [Online]. Available: http://jcp.org (downloaded 2013, Sep. 10)

[4] Android NFC API. (2013). Developer Reference [Online]. Available: http://developer.android.com (downloaded 2013, Sep. 10)

[5] K. Choi, J. Kim, and S. Park, "A Secure Application Invocation Mechanism in Mobile Phones for NFC," *IEEE Int'l Conf. on Consumer Electronics*, pp.737-738, Las Vegas, USA, Jan. 13th, 2012.

[6] NFC Forum. (2006, Jul 24). URI record type definition technical specification [Online]. Available: http://www.nfc-forum.org/home/ (downloaded 2013, Sep. 10)

[7] NFC Forum. (2006, Jul 24). Text record type definition technical specification [Online]. Available: http://www.nfc-forum.org/home/ (downloaded 2013, Sep. 10)

[8] NFC Forum. (2006, Jul 24). Smart poster record type definition technical specification [Online]. Available: http://www.nfc-forum.org/home/ (downloaded 2013, Sep. 10)

[9] NFC Forum. (2006, Jul 24). Generic control record type definition technical specification [Online]. Available: http://www.nfc-forum.org/home/ (downloaded 2013, Sep. 10)

[10] R. Kelsey, W. Clinger, and J.Rees (eds.), "The Revised5 Report on the Algorithmic Language

Scheme," *Higher-Order and Symbolic Computation*, vol.11, no.1, August, 1998.
[11] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "Practical NFC peer-to-peer relay attack using mobile phones," *Int'l Conf. on Radio Frequency Identification: Security and Privacy Issues*, pp.35-49, Springer, Berlin Heidelberg, 2010.
[12] G. Madlmayr., J. Langer, C. Kantner, and J. Scharinger, "NFC devices: Security and privacy," *IEEE 3rd Int'l Conf. on Availability, Reliability and Security*, pp.642-647, Washington, DC, USA, 2008.
[13] E. Haselsteiner and K. Breitfuß, "Security in near field communication (NFC)," *Workshop on RFID Security*, Graz, Austria, Jul. 2006.
[14] George C. Necula, Compiling with Proofs, Ph.D. thesis, School of CS, CMU, Sept. 1998.

고 명 필
2013년 연세대학교 컴퓨터공학과 졸업(공학사). 2013년~현재 연세대학교 전산학과 석사과정. 관심분야는 모바일 소프트웨어, 프로그래밍언어, 컴파일러, 프로그램 분석, 소프트웨어 검증

최 광 훈
1994년 한국과학기술원 전산학과 졸업(학사). 1996년 한국과학기술원 전산학과 졸업(공학석사). 2003년 한국과학기술원 전산학과 졸업(공학박사). 2003년~2005년 JAIST, Researcher. 2005년~2006년 Tohoku Univ., Researcher. 2006년~2010년 LG전자 Mobile Communication 연구소, 책임연구원. 2010년~2011년 서강대학교 컴퓨터공학과 BK21연구교수. 2011년~현재 연세대학교 컴퓨터정보통신공학부 조교수 관심분야는 모바일 소프트웨어, 프로그래밍언어, 컴파일러, 프로그램 분석

임 효 상
1998년 연세대학교 컴퓨터과학과 졸업(학사). 1999년 한국과학기술원 전산학과 졸업(석사, 박사). 2007년~2011년 미국 Purdue Univ. Computer Science Department 박사후 연구원. 2011년~현재 연세대학교 컴퓨터정보통신공학부 조교수. 관심분야는 모바일 데이터베이스, 데이터스트림, 정보보안, 데이터 신뢰도 분석, GPU를 사용한 데이터처리