MAC 주소를 이용한 NFC 릴레이 공격의 방어기법

오성택, 강석인, 홍만표
아주대학교 일반대학원 컴퓨터공학과
e-mail : angelrick@ajou.ac.kr
e-mail : kingksi@ajou.ac.kr
e-mail : mphong@ajou.ac.kr

Countermeasure of Relay Attack based on NFC with MAC Address

Sungtaek Oh , Sukin Kang, Manpyo Hong
Ajou University

요 약

NFC 디바이스의 보급화로 기존의 결제서비스보다 편리한 NFC 결제 서비스의 활성화가 예상된다. 하지만 편리성이라는 장점에만 집중하여 이를 뒷받침해줄 보안서비스가 제공되지 않는다면 득보단 실이 많은 서비스가 될 것이다. 실제로 NFC 서비스의 경우 릴레이 공격에 취약한 모습을 보이는데 릴레이 공격은 원리와 구현이 간단하여 향후 NFC 서비스가 상용화될 경우 악용될 염려가 많다. 본 논문에서는 NFC 서비스의 가장 큰 보안위협인 릴레이공격에 대한 방어기법으로 NFC 디바이스의 MAC 주소를 이용한 다중 요소 인증방법을 제안한다.

1. 서론

스마트 디바이스가 확산되면서 생활에 밀접한 어플리케이션과 서비스 개발이 급격하게 증가하고 있다. NFC(Near Field Communication)는 비접촉식 근거리 무선 통신 기술로 13.56 MHz 의 주파수대역을 이용하여 약 4cm 이하의 근거리통신을 하며 0.1 초 이내의 인식 속도, 106-848Kbps 의 데이터 전송 속도를 지원하며 NFC 디바이스간 또는 NFC 디바이스와 리더기 간에 정보를 송수신한다[1]. NFC 는 ECMA(European Computer Manufacturers Association), ISO(International Organization for Standardization), ETSI(European Telecommunications Standards Institute)에서 표준을 진행하고 있다. NFC 기술은 카드 에뮬레이션 모드, 단말대 단말 모드, 읽기/쓰기 모드 총 3 가지 운용모드가 존재하며[2] 모바일 결제, 티켓팅, 스마트포스터 등과 같은 다양한 서비스를 제공한다. 2009 년 이후 출시된 스마트 디바이스에 NFC 기능이 탑재되면서 NFC 기반 서비스가 주목을 받기 시작하였다. 국내경우 2012 년 11 월 통신사와 카드사, VAN(Value-Added Network)사 등이 연합하여 명동에 NFC 시범사업을 추진하였고 2013 년 5 월 여수엑스포에서 NFC 서비스를 운영하고 있다. 해외에서는 구글사의 구글 월렛 서비스를 2011 년 9 월 상용화하여 현재 모바일 결제 서비스를 중심으로 사업을 추진 중에 있다. 이러한 NFC 모바일 결제 서비스가 확산되면서 기존의 신용카드를 이용한 결제에서 좀 더 간편한 스마트 디바이스를 이용한 결제로의 변화가 예상된다[3]. 하지만 편리성이라는 장점에만 집중하여 보안성을 고려하지 않을 경우 사용자가 입는 피해가 클 수 있기 때문에 관련 서비스의 취약점과 보안 위협을 파악하고 해결하여야 한다. 해외에서 상용화가 되고 있는 구글 월렛 서비스가 릴레이 공격에 취약하다[4]는 문제점이 보고되면서 릴레이 공격에 대한 방어기법 마련이 중요하다. 본 논문에서는 이러한 NFC 의 알려진 보안 위협에 대해 파악하고 그 중 릴레이 공격에 대한 자세한 방어기법을 제안한다.

본 논문의 구성은 다음과 같다. 2 장에서는 본 논문에서 다룰 NFC 에 대한 공격유형과 방어기법을 살펴보고, 3 장에서는 본 논문에서 제안하는 릴레이공격에 대한 방어대책에 대해서 설명한다. 5 장에서는 제안내용에 대한 분석과 5 장에서는 결론을 기술한다.

2. NFC 공격유형과 방어기법

2.1. 릴레이공격

그랜드 마스터 체스 문제[6]는 릴레이 공격의 전형적인 예를 제공한다. 체스 게임의 룰을 모르는 플레이어가 두 명의 체스 그랜드 마스터 사이에서 각각의

그랜드 마스터의 말의 이동을 따라 하면 각각의 그랜드 마스터는 플레이어가 게임을 하고 있는 것으로 알지만 실상은 그렇지 않다. 이 같은 공격을 NFC 시스템에 적용할 경우 어떠한 보안 프로토콜이 있어도 공격자는 요청과 응답을 전달만 하면 되기 때문에 공격이 간단하다[7]. 릴레이 공격은 어플리케이션 계층에서의 암호화로는 현재 방어할 수 없다[8, 9]. [그림 2]는 실제 NFC 서비스에서 가능한 릴레이공격이다. 공격자 Ma 와 공격자 Mb 는 사용자와 결제리더기 사이에서 메시지 전달만으로 공격을 성공할 수 있다.

[그림 1] 릴레이공격

2.2. 방어기법

릴레이공격의 경우 메시지가 전달되었다가 돌아오는 시간을 측정하여 탐지하는 거리 제한(Distance bounding) 프로토콜 방식, 위치를 이용하여 탐지하는 방식 그리고 소리를 이용한 탐지방식이 있다[10, 11, 12]. 하지만 경계거리 프로토콜의 경우 공격자가 유선채널을 이용하게 되면 빠르게 메시지를 전달할 수 있게되어 탐지가 어렵다[13]. 위치를 이용하는 방식은 두 디바이스가 각각의 위치를 측정하고 비교하여 인접함을 증명하는 방식이다. 그러나 현재 대표적인 위치 측정 기술인 GPS(Global Positioning System)는 실내에서의 정확도가 상당히 낮고 오류의 발생빈도가 높다[14]. 본 논문에서는 사용자의 보안성을 최대한 보장할 수 있는 아이디어를 제안한다.

3. 제안

사용자 A 는 카페에서 커피를 구매하고 NFC 를 이용하여 간단하게 결제를 한다. 정상적인 경우라면 사용자 A 의 NFC 디바이스로 직접 카페의 결제리더기에 결제를 요청하여야 한다. 하지만 공격자 Ma 와 공격자 Mb 는 이러한 사용자 A 의 NFC 디바이스를 릴레이공격으로 자신들의 커피를 결제하려고 한다[그림 2]. 공격자 Ma 와 공격자 Mb 의 디바이스는 NFC 기능이 탑재된 디바이스이며 별도의 통신채널을 가지고 있다고 가정한다. 공격자 Mb 는 카페의 결제리더기에 결제를 요청한다. 공격자 Mb 는 결제리더기로부터 받은 결제정보요청 메시지를 공격자 Ma 에게 전달하여 공격자 Ma 가 사용자 A 에게 결제정보요청 메시지를 전달한다. 사용자 A 의 디바이스는 결제정보요청에 대한 응답으로 결제정보 메시지를 공격자 A 에게 전달하게 되고 공격자 Ma 는 공격자 Mb 에게 결제정보 메시지를 전달한다. 공격자 Mb 는 전달받은 메시지를 결제리더기에게 전송하여 결제를 요청한다. 결제리더기는 사용자 A 의 결제요청으로 인식하고 결제를 승인한다. NFC 의 특성상 인증을 요청하는 디바이스와 인증을 받는 기기는 매우 가까이에 위치해야 하지만 릴레이 공격은 단순한 메시지 전달만으로 이루어 지기 때문에 원거리에 위치한 NFC 디바이스도 정상적인 사용자의 디바이스인 것처럼 인증을 요청할 수 있다. 그렇기 때문에 인증을 요청하는 디바이스가 인증시스템과 가까이에 위치한 정상 디바이스 라는 것을 입증하여야 한다. 본 논문에서는 NFC 디바이스의 고유 MAC 주소를 이용한 다중 요소 인증을 제안한다. 인증절차는 다음과 같이 진행되며 최종결제승인을 하기 전에 이루어진다.

1. 인증시스템은 인증을 요청한 디바이스(사용자 A)에게 인증요청메시지를 전송한다. 인증요청메시지에는 인증시스템이 관리하는 무선보안채널의 SSID(Service Set Identification)와 비밀번호를 포함한다.
2. 사용자 A 는 인증시스템이 요청한 무선보안채널에 접속한 후 인증시스템으로 접속완료메시지를 전송한다. 접속완료메시지에는 디바이스의 MAC 주소를 포함한다.
3. 인증시스템은 전달받은 MAC 주소와 무선보안채널에 접속한 디바이스의 MAC 주소를 비교한 후 일치하면 인증, 아니면 거부한다.
4. 인증이 성공했다면 사용자 A 는 최종결제를 진행한다.

인증에 사용된 무선보안채널의 연결정보는 사용자 A 의 디바이스에 저장되지 않으며, 인증시스템의 무선보안채널정보(SSID, 비밀번호) 는 주기적으로 변경된다. 인증과정진행 중 공격자에 의해 메시지가 누락되면 인증은 취소된다. 사용자 A 와 인증시스템이 가까이에 위치해 있다면 인증시스템의 무선보안채널에 접속할 수 있고 MAC 주소 비교를 통해 인증을 성공할 수 있다.

[그림 2] MAC 주소를 이용한 인증방식

본 제안에서는 총 3 번의 NFC 태깅이 이루어진다. 첫 번째 태깅은 사용자 A 가 결제리더기에 결제를 요청할 때 수행되며, 두 번째 태깅은 사용자 A 가 인증

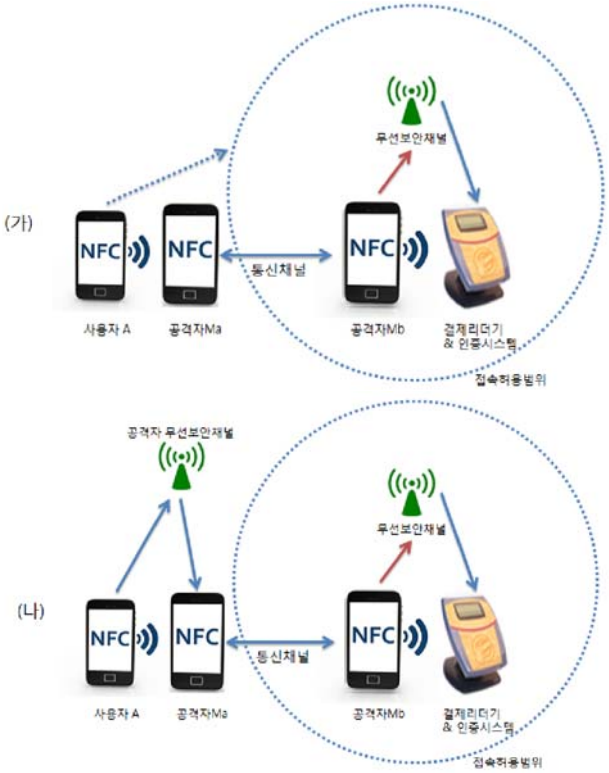
시스템의 무선보안채널에 접속한 후 MAC 주소를 전송하기 위해서 수행된다. 마지막 태깅은 인증이 완료된 후 최종결제를 위해서 수행된다. 기존의 NFC 서비스의 결제방식에는 한번의 태깅으로 가능하지만 본 논문에서는 MAC 주소를 이용한 다중 요소 인증으로 인해 태깅 횟수가 증가된다.

4. 보안분석

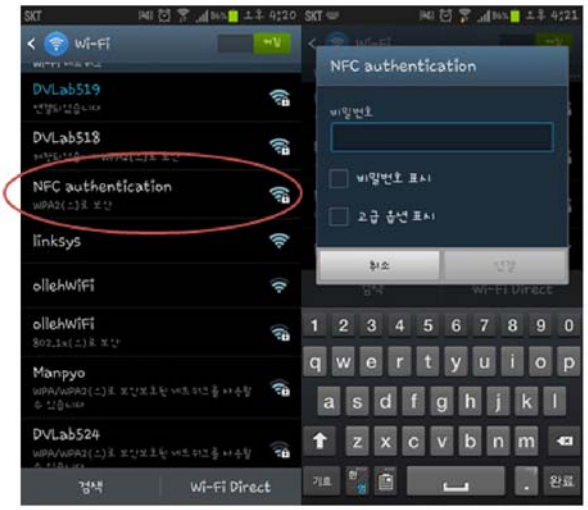
[그림 3]는 실제 발생 가능한 릴레이공격의 공격모델이다. 공격자 Ma 와 공격자 Mb 의 디바이스는 NFC 기능이 탑재되어 있고 서로 통신이 가능한 채널을 가지고 있다. 사용자 A 의 디바이스에는 시스템권한을 획득할 수 있는 악성 코드나 어플리케이션이 설치되어 있지 않고 공격자가 시스템을 제어할 수 없다고 가정하였다. [그림 3](가)의 경우 사용자는 인증시스템의 무선보안채널의 접속허용범위를 벗어나 있어 접속을 할 수 없다. 접속을 완료할 수 없어 사용자 A 는 MAC 주소를 전송하지 않고 인증은 실패하게 된다. [그림 3](나)의 경우처럼 사용자 A 가 접속허용범위 밖에 있지만 공격자 Ma 가 공격자무선보안채널을 만든 경우 [그림 4]와 같이 사용자가 무선보안채널에 직접 연결을 해야 한다. 공격자 Ma 가 사용자 A 의 디바이스를 조작할 수 없기 때문에 [그림 3](나)공격모델 B 의 경우에도 인증과정을 마무리 하지 못하여 인증을 실패하게 된다. 제안방식으로 증명하려는 것은 디바이스의 MAC 주소를 이용하여 두 디바이스가 인접하여 있는지 파악하여 릴레이공격에 대한 방어를 할 수 있다는 것이다. 두 NFC 디바이스의 인증 과정 중 인증을 요청한 디바이스를 인증시스템의 무선보안채널에 접속할 수 있게 하여 접속한 디바이스의 MAC 주소와 인증 요청 디바이스가 전송한 MAC 주소가 일치하는지를 기준으로 인증 가능여부를 확인한다. 이 경우 릴레이공격을 탐지할 수 있는지가 주요 평가기준이며, 릴레이공격에 의한 인증의 경우 [그림 3](가)같이 정상사용자의 디바이스가 인증시스템의 무선보안채널의 접속허용범위를 벗어날 경우 MAC 주소 전송이 이루어지지 않는다. [그림 3](나)와 같이 공격자 무선보안채널로 접속을 유도하여도 [그림 4]와 같이 사용자의 조작 없이는 무선보안채널에 접속할 수 없기 때문에 릴레이공격은 실패한다.

5. 결론

NFC 서비스 에서의 릴레이 공격은 단순한 메시지 전달만으로 멀리 떨어져있는 두 정상기기의 정상인증을 시도할 수 있는 공격기법이다. 릴레이 공격을 방어하기 위해서는 현재 인증을 요청하는 디바이스와 인증시스템이 가까운 거리에 있다는 것을 증명해야 한다. 경계거리 프로토콜의 경우 통신기술의 발달로 정확한 탐지가 어렵다. 위치정보를 이용한 방식 또한 측정기술의 정확도와 높은 오류빈도로 탐지에 어려움이 있다. 본 논문은 릴레이 공격에 방어하기 위해서 다중 요소 인증을 제안하고 인증 요소로 디바이스의 MAC 주소를 이용하였다. 인증시스템이 요청하는 무선 네트워크에 접속하기 위해서는 해당 네트워크의 범위 내에 사용자의 디바이스가 있어야 하며 공격자가 인증을 위한 무선 네트워크에 접속하여도 사용자와 공격자의 MAC 주소가 달라 공격자의 인증시도는 실패하게 된다.



[그림 3] (가) 공격모델 A
(나) 공격모델 B



[그림 4] 무선보안채널 연결

Acknowledgement

이 논문은 2013 년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2011-0011289)

참고문헌

[1] NFC Forum, Available: http://www.nfc-forum.org
[2] GSMA "mobile NFC Service V1.0" 2007
[3] 백종현, 염흥열, "NFC 기반 모바일 서비스 보안 위협 및 대책," 한국정보보호학회 23(2), pp. 55-59, 2013 년 4 월.
[4] Michael Roland and Josef Langer, "Applying Relay Attacks to Google Wallet," NFC Research Lab Hagenberg, Feb. 2013.
[5] Henning Siitonen Kortvedt and Stig F. Mjolsnes, "Eavesdropping Near Field Communication," The Norwegian Information Security Conference (NISK), 2009.
[6] J. H. Conway, "On numbers and Games," Academic Press. 1976.
[7] Zhao Wang, Zhigang Xu, Wei Xin and Zhong Chen, "Implementation and Analysis of a Practical NFC Relay Attack Example," Second International Conference on Instrumentation & Measurement, Computer, Communication and Control, 2012.
[8] G. P. Hancke, "A Practical Relay Attack on ISO 14443 Proximity Cards," (Retrieved: 20 Sep 2011), Jan. 2005.
[9] G. P. Hancke, K. E. Mayes, and K. Markantonakis, "Confidence in smart token proximity: Relay attacks revisited," Computers & Security, 28(7):615-627, 2009.
[10] Z. Kfir and A. Wool, "Picking Virtual Pockets using Relay Attack on Contactless Smartcard," In Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM' 05), pp.47-58, Sep. 2005.
[11] S. Brands and D. Chaum. "Distance-Bounding Protocols (Extended Abstract)," Advances in Cryptography EUROCRYPT '93. LNCS 765, pp. 344-359. May 1993.
[12] 김종욱, 강석인, 홍만표, "소리를 이용한 릴레이공격 공격의 탐지," 한국정보보호학회 23(4), pp. 617-627, 2013 년 8 월
[13] P. Thevenon, O. Savry, and S. Tedjini, "On the weakness of contactless systems under relay attacks," Software, Telecommunications and Computer Networks (SoftCOM), 19th International Conference, pp. 1-5, Sept. 2011.
[14] T.D. Le, T.M. Doan, H.N. Dinh, and N.T. Nguyen, "ISIL: Instant search-based indoor localization," IEEE Consumer Communications and Networking Conference (CCNC), pp. 143-148, Jan. 2013.