한국컴퓨터정보학회 하계학술대회 논문집 제18권 제2호 (2010. 7)

Jini 2.x 보안 모델을 응용한 스마트폰 응용의 안전한 푸시 서비스

지형준°, 최재영*, 김성기**, 민병준*
°*인천대학교 컴퓨터공학과
**선문대학교 IT교육학부
e-mail: {nanjanu, jero}@incheon.ac.kr, skkim@sunmoon.ac.kr, bjmin@incheon.ac.kr

The Trusted Push Service Scheme of Smartphone Using Jini 2.x Standard Security Model

Hyeong-Jun Ji°, Jae-Yeong Choi*, Sung-Ki Kim**, Byeong-Joon Min*
°*Dept. of Computer Science and Engineering, Incheon University
**IT Education Center, Sun-Moon University

● 요 약 ●

본 논문에서는 Jini 2.x 표준 보안 모델을 활용하여 모바일 기기의 신뢰성 있는 푸시 서비스 방안을 제안한다. Jini 시스템은 유비쿼터스 네트워크 환경에서 서버와 클라이언트를 연결하는 기술이다. 또한 안전한 시스템 구성을 위해서 Jini 2.x 표준 보안 모델을 마련하여 보안을 강화하였다. 푸시 서비스는 사용자가 서버에 서비스를 등록하면 서버에서 각 사용자의 모바일 기기에 데이터를 전송한다. 이 푸시 서비스는 앞으로 많은 비즈니스 모델을 만들 것으로 예상된다. 하지만 푸시 방식은 풀 방식에 비해 많은 보안 문제를 발생시킬 것이다. 본 논문에서는 이전의 신뢰성 있는 푸시 서비스를 위한 방안과 Jini 2.x 표준 보안 모델이 어떻게 안전한 푸시 서비스를 제공할 수 있는지 살펴본다.

키워드: 푸시(push), 푸시 서비스, 푸시 보안

I. 서론

스마트폰을 일반폰과 구별 짓는 가장 큰 특성은 개방성이다[1]. 스마트폰은 범용 운영체제를 사용하고, 표준화된 개발 환경을 제공하여 개방화된 운영체제를 통해 개발자들이 자유롭게 애플리케이션을 개발할 수 있는 환경을 제공한다. 이렇듯 누구나 콘텐츠를 제작하거나 배포가 가능하기 때문에 악성코드가 포함된 애플리케이션의 제작 및 유포도 가능하다. 최근의 스마트폰의 증가로 인해 보안 위협도 증가할 것으로 예측된다. 이로써 현재 스마트폰에 대한 다양한 보안 위협과 대응기술들이 연구되고 있다[2]. 스마트폰의 취약점은 대부분 컴퓨터의 그것과 비슷할 것으로 예상되지만, 스마트폰이 지극히 개인적인 기기라는 점에서 다른 위협도 분명히 존재한다.

푸시 서비스는 원하는 정보를 찾아 내려받는 '풀(Pull)'방식이 아니라, 서비스 제공자가 콘텐츠를 사용자의 스마트폰으로 전송해 주는 방식이다. 이 서비스가 사용되는 분야는 e메일, 소프트웨어 업그레이드, 미디어, 멀티미디어 콘텐츠 등이다. 하지만 푸시 서비스는 편리한 서비스인 반면에, 보안 위협에 쉽게 노출될 수 있다. 해당 푸시 메시지가 악성코드를 포함하고 있다거나, 출처를 알 수 없는 곳으로 사용자의 접속을 유도할 수도 있기 때문이다. 본 논문에서는 Jini 2.x 표준 보안 모델을 활용하여 신뢰성 있는 스마트폰의 푸시 서비스 방안을 제시한다. 2장에서는 푸시 서비스 보안에 대한 기존의 연구 내용을 소개한다. 3장에서는 Jini 2.x 표준 보안 모델을 설명하고, 신뢰성 있는 푸시 서비스에 어떻게 적용할 수 있는지 설명한다. 그리고 4장에서 결론을 맺는다.

II. 관련 연구

1. 관련연구

Callback URL SMS 기술은 사용자가 메시지의 연결 버튼을 누르면 특정한 URL로 연결이 되도록 한다. 이 기술은 사용자가 URL을 입력하는 수고를 덜 수 있기 때문에, 앞으로 많이 쓰일 것으로 기대된다. 하지만, Callback URL이 올바른지 보장할 수가 없다는 취약점이 있다. 실제로 URL-SMS 스팸공격이 발생했다. 사용자는 SMS가 포함하고 있는 악의적인 Callback URL을 구별해 낼 수가 없다. 이러한 보안 문제를 해결하기 위해서 메시지와 함께 공개키, 비밀키, 세션정보 같은 보안 앨리먼트를 추가한다[3]. [4]은 CDMA 무선 네트워크상의 PDA를 위한 안전한 푸시 서비스 모델을 제안하고 구현한다. 제안하는 보안 프로토콜은 초기 등록 단계, 비표(nonce table) 생성 단계, 푸시 서비스의 3단계로 나뉜다. 초기 등록 단계에서는 서버와 클라이언트가 공개키와 비밀키를 교환하고, 비표 생성 단계는 안전한 세션키를 생성하기 위해 비표를 64개 만든다. 푸시 서비스 단계는 속도를 향상시키기 위해

준비된 비표를 사용하고 안전한 통신을 위해 비표의 번호는 SMS 채널을 이용하고 푸시 데이터는 데이터 채널을 이용한다.

TCG(Trusted Computing Group)에서는 하드웨어 기반의 신뢰성 있는 컴퓨팅 환경을 위해서 TPM(Trusted Platform Module)과 모바일 환경에 적합한 MTM(Mobile Trusted Module)의 사용을 제안하고 있다[5]. MTM은 하드웨어 구성과 소프트웨어 상태를 점검할 수 있는 PCR(Platform Configuration Register)을 가지고 있어 플랫폼에 대한 무결성 검사 와 인증을 수행한다. 외부로부터 인증된 2048비트의 개인키와 공개키를 가지고 있고, 이러한 키는 내부의 안전한 저장소에 저장되어 보호된다. [6]는 이러한 신뢰 컴퓨팅 기술을 기반으로 안전한 푸시 서비스를 2가지 방식으로 제안하고 있다.

III. 본론

1. Jini 서비스 환경

Jini 시스템의 동작은 그림2처럼 서비스 제공자가 Lookup 서비스를 탐색하는 과정, 서비스 제공자가 Lookup 서비스에 자신의 서비스를 등록하여 Jini 네트워크에 합류하는 과정, 클라이언트가 서비스를 사용하기 위해서 서비스 프락시를 다운로드 받는 과정, 클라이언트가 자신이 사용하고자 하는 서비스를 사용하는 서비스 수행과정으로 나뉜다.

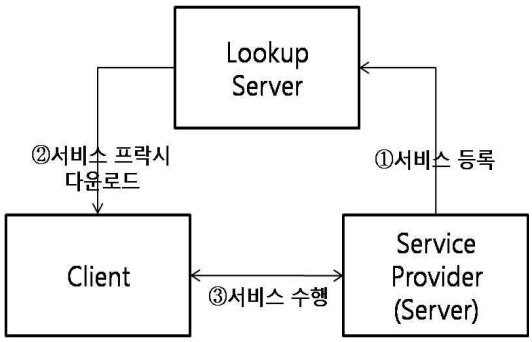

그림 2. Jini 서비스 환경
Fig. 2. Jini Service Environment

서버는 자신의 서비스를 Lookup 서버에 등록시키기 위해서 디스커버리 프로토콜을 사용하여 Lookup 서버의 위치를 발견하고, 클라이언트는 서비스 프락시를 다운받기 위해서 디스커버리 프로토콜을 사용하여 Lookup 서버의 위치를 발견해야 한다. 발견 이후에 서버는 자신의 서비스를 Lookup 서버에 등록하고 클라이언트는 Lookup 서비스 프락시를 통해서 이용 가능한 서비스를 발견한다. 클라이언트가 원하는 서비스를 선택하면 해당 서버가 제공한 서비스 프락시를 Lookup 서버로부터 받게 되고, 이를 이용해서 원격의 서비스 구현을 호출한다[7].

2. Jini 2.x 표준 보안 모델

기존의 Jini 시스템에 대한 보안성을 향상시키기 위해 많은 연구들이 있었는데, 이들 연구에서 공통적으로 제시한 보안요구 사항들은 다음과 같다.

- 클라이언트, 서비스 프락시, 서버 간의 신뢰확립
- 서비스 접근 제어
- 이동 코드로부터 클라이언트 보호
- 통신채널의 기밀성과 무결성 보장

클라이언트, 서버, 서비스프락시 간의 신뢰 요구사항은 상호 접근에 대한 인증 메커니즘의 필요성을 의미한다. 또한 서비스 접근 제어는 인증과 연결하여 권한에 따라 서비스 접근을 제어하는 인가 방법의 필요성을 의미한다. 그리고 이동코드로부터 클라이언트를 보호하는 것은 인증받은 서비스프락시 코드라고 해도 그 코드의 수행이 클라이언트에게 해를 주지 않도록 제약하는 방안이 필요하다는 것을 의미한다. 마지막 보안요구는 필요한 모든 메시지 교환에 기밀성과 무결성을 제공해야함을 의미한다. Jini 2.x에서는 이러한 모든 보안 요구사항을 충족시키기 위해 보완되었다.

실제로 서비스 제공자와 클라이언트간의 통신을 수행하는 것은 프락시 객체이다. 여기서 2가지 문제점이 발생한다. 첫 번째는 클라이언트가 다운로드 받은 서비스 프락시가 인증되지 않은 출처로부터 유입될 수도 있다는 것이다. 두 번째는 프락시 객체가 클라이언트에서 잘못된 서비스를 실행할 수 있다는 것이다. 그렇기 때문에 서비스 프락시의 출처를 확인하고 신뢰할 수 있는지를 확인해야 한다. 다음 그림3은 프락시의 신뢰 검증 단계이다.

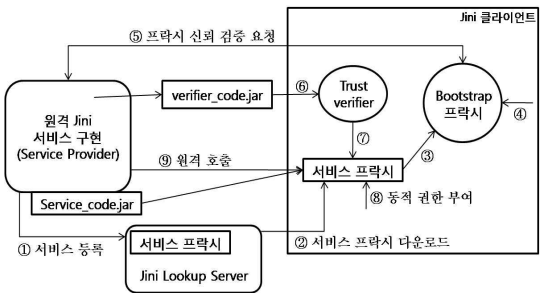

그림 3. 프락시 신뢰 검증 단계[8]
Fig. 3. proxy trust verification stage

① 서비스 등록 : 서비스 제공자는 자신이 제공하고자 하는 서비스 목록 및 서비스에 필요한 데이터 인스턴스들과 관련 클래스 파일들의 위치를 알려주는 URL과 이 URL로부터 추출한 해시값을 포함시켜서 Jini Lookup 서비스의 서비스 프락시에 등록을 시킨다.

② 서비스 프락시 다운로드 : 클라이언트가 서비스를 사용하기 위해서 Jini Lookup 서비스로부터 서비스에 필요한 데이터 인스턴스 및 관련 클래스 파일의 URL과 서버 측 제약이 설정된 서비스 프락시를 다운로드 한다.

③ Bootstrap 프락시 : 클라이언트는 다운로드 받은 서비스 프락시가 서비스 제공자가 등록시킨 서비스 프락시가 맞는지 검증해야 한다. 이를 위해서 Jini 클라이언트는 다운받은 서비스 프락시로부터 클라이언트 로컬에 완전히 신뢰할 수 있는 코드를 이용하여 Bootstrap 프락시를 생성한다.

④ 클라이언트는 ③에서 생성한 Bootstrap 프락시에 클라이언트에 필요한 보안 요구사항인 제약을 설정하고 실행시킨다.

⑤ 프락시 신뢰 검증 요청 : Bootstrap 프락시는 서비스 제공자로부터 다운로드된 서비스 프락시가 실제 서비스 제공자로부터 전송되어진 서비스 프락시가 맞는지 확인하기 위해서 신뢰 검증자 객체를 이용하여 원격 콜백(call back) 메소드를 호출한다.

⑥ 신뢰 검증자 전송 : 서비스 제공자는 클라이언트가 다운로드된 서비스 프락시를 검증할 수 있도록 신뢰 검증자 객체가 포함된 verifier_code.jar 파일을 전송한다. 이 신뢰 검증자에는 지켜져야 할 규칙에 의거하여 다운로드된 프락시에 대한 인스턴스를 포함하고 있다.

⑦ Jini 클라이언트 신뢰 검증자에 포함된 다운로드 받은 프락시에 대한 인스턴스와 다운로드 받은 프락시를 비교하고 일치한다면 이 다운로드 받은 프락시를 신뢰할 수 있다고 판단한다.

⑧ 검증된 서비스 프락시에 서비스 제공자에서 각 클라이언트마다 적용되는 신뢰 등급에 따라서 동적으로 권한을 부여한다.

⑨ 서비스 프락시에 클라이언트를 보호할 수 있는 제약을 새롭게 설정하고 원격으로 통신을 한다.

3. 푸시 서비스의 보안 위협

푸시서비스를 이용하기 위해서는 해당 서비스에 등록하거나 푸시 서비스를 제공하는 애플리케이션을 스마트폰에 설치해야 한다. 현재 푸시 서비스를 가장 잘 활용하는 분야는 e메일 서비스와 애플리케이션 업그레이드, 블로그나 카페 등의 새로운 글을 알릴 때, 미디어나 멀티미디어 콘텐츠의 전달의 경우이다. 이러한 경우의 푸시 서비스의 보안 요소는 5가지 정도로 제시할 수 있다. 첫 번째는 전송중인 푸시 메시지의 기밀성과 무결성이 보장되어야 한다. 두 번째는 푸시 메시지가 올바른 출처에서 왔는지를 확인해야 한다. 잘못된 출처에서 온 메시지를 아무런 의심없이 확인하여 해당 URL로 접속이 된다면 악성코드에 감염될 수 있다. 세 번째는 푸시 메시지가 올바르게 만들어졌는가를 확인하는 것이다. 푸시 메시지 자체에 스마트폰의 API를 실행시켜 악성코드에 감염시킬 수 있기 때문이다. 네 번째는 스팸성 푸시를 차단해야 한다. 현재 사용하고 있는 문자메시지도 하루에 수십 개의 스팸문자가 오는 경우가 있다. 사용자가 직접 등록한 푸시 서비스가 아닐 경우에는 받지 말아야 한다. 다섯 번째는 자신의 푸시 메시지를 다른 사람이 받아볼 수 있다는 것이다.

이런 문제를 해결하기 위해서는 Jini 2.x 보안 모델과 마찬가지로 해당 푸시 메시지가 올바른 경로에서 왔는지와 메시지를 신뢰할 수 있는지를 먼저 확인해야 한다.

4. 안전한 푸시 서비스 방안

Jini 2.x 모델에서 서버는 서비스 제공자이고 푸시 서비스를 제공하는 업체라고 할 수 있다. 또한 클라이언트는 푸시 서비스를 제공받는 스마트폰의 소유자이다. 그리고 Lookup 서버는 최초 클라이언트가 푸시 서비스를 신청하는 단계라고 할 수 있다.

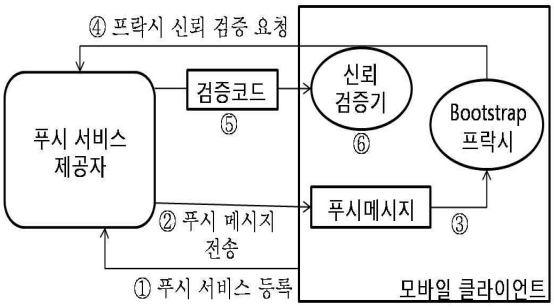

그림 3. 푸시 서비스 신뢰 검증 단계
Fig. 3. push service trust verification stage

① 푸시 서비스 등록 : 푸시 서비스를 이용하기 위해서는 먼저 클라이언트가 해당 서비스에 등록해야 한다. 등록과정에서 클라이언트는 서비스 제공자의 URL의 해시값을 저장한다.

② 푸시 메시지 전송 : 서비스 제공자는 새로운 데이터가 있을 경우 클라이언트에 푸시 메시지를 전송한다. 이때 클라이언트는 받은 푸시 메시지의 출처를 확인하기 위해서 URL의 해시 값을 ①에서 저장해놓은 해시값과 비교하여 올바른 출처에서 온 것인지를 확인한다.

③ 푸시 메시지 자체가 올바른지 확인하기 위해서Bootstrap 프락시를 만든다.

④ 서비스 제공자에게 푸시 메시지가 신뢰적인지 확인하기 위해서 검증 코드를 요청한다.

⑤ 서비스 제공자는 해당 검증 코드를 클라이언트에 전송한다.

⑥ 클라이언트의 신뢰 검증기는 서비스 제공자에 요청한 신뢰 코드를 이용하여 푸시메시지의 신뢰 여부를 판단한다.

Ⅳ. 결론

푸시 서비스는 사용자의 의지없이 자동적으로 사용자에게 콘텐츠를 제공한다는 점에서 유비쿼터스적인 요소를 지니고 있는 서비스이다. Jini 2.x 표준 보안 모델도 역시 유비쿼터스 환경에서 취약할 수 있는 Jini 시스템의 보안 요구 사항을 충족시키기 위해 제안되었다. 그렇기 때문에 신뢰성 있는 푸시 서비스를 위해서 Jini 2.x 표준 보안 모델을 활용하는 것이 적당할 것으로 생각된다. 그러나 본 논문은 스마트폰의 다양한 플랫폼 환경을 고려하지 않았다. Jini 시스템은 Java 기반으로 모든 시스템에 적용이 가능하지만 성능이 낮은 스마트폰에서는 무리일 수 있다. 그러므로 향후 스마트폰의 다양한 플랫폼 환경에서도 적용이 가능한 적용 방안에 대한 연구가 필요하다.

참고문헌

[1] 김기영, 강동호, "개방형 모바일 환경에서 스마트폰 보안기술", 정보보호학회지, 제19권, 제5호, pp.21-28, 2009.10.

[2] 강동호외, "스마트폰 보안 위협 및 대응 기술", 전자통신동향분석, 제25권, 제3호, pp.72-80, 2010.06.

[3] Seung-Hyun Kim, Seunghun Jin, "Security-Enhanced Callback URL Service in Mobile Device", The 9th International Conference on, 2007.02.

[4] Jeong Kyoon Lee, Ki young Lee, "The Implementation of Security Message Protocol for PDA PUSH Service", TENCON 2005 2005 IEEE Region 10, 2005.

[5] TCG Mobile Trusted Module, Specication v. 1.0, revision 1, 12 June 2007, https://www.trustedcomputinggroup.org/specs/mobilephone/tcg-mobile-trusted-module-1.0.pdf

[6] Nicolai Kuntze, Andreas U. Schmidt, "Trustworthy content push", WCNC 2007, 2007.

[7] Peer Hasselmeyer, et al., "Trade-offs in a Secure Jini Service Architecture", LNCS 1890, Springer-Verlag Berlin, 2000.

[8] Sun Microsystems, "Jini Technology Starter Kit Overview v2.0", Published Specification, http://java.sun.com/developer/products/jini/arch2_0.html, 2003.