모바일 웹서비스 메시지의 보안 평가에 관한 연구

이성현* · 이재승*

*한국전자통신연구원 홈네트워크보안연구팀

A Study on Security Evaluation for Mobile Web Services Message

Seoung-Hyeon Lee* · Jae-Seung Lee**

*Home Network Security Research Team, ETRI

E-mail : duribun@etri.re.kr

요 약

본 논문에서는 모바일 웹서비스 메시지에 대한 보안 수준을 측정하고, 보안성과 신뢰성을 향상시키기 위한 방법으로, 모바일 웹서비스 메시지에 대한 보안 평가 방안을 제시하였다. 본 논문에서는 이를 위해서 모바일 웹서비스 보안 서비스의 개요와 보안 위협을 정의한 후, 모바일 웹서비스 메시지 보안 평가 방법을 정의하였다. 또한, 모바일 웹서비스 메시지 보안 평가를 위한 요구사항들을 정의하였고, 모바일 웹서비스 메시지 보안 평가 프레임워크를 구성하였다. 마지막으로, 모바일 웹서비스 메시지 보안 평가 프레임워크를 이용한 평가 시나리오에 대한 예제를 제시하였다. 본 논문에서 제시한 모바일 웹서비스 메시지 보안 평가 방안을 통해서, 모바일 웹서비스가 제공되기 이전에 모바일 웹서비스 메시지에 대한 보안 수준을 점검할 수 있으며, 발생할 수 있는 보안 위협에 대한 대응책을 마련할 수 있다. 이를 통해서, 모바일 웹서비스 메시지에 대한 보안성과 신뢰성을 향상시킬 수 있고, 모바일 웹서비스의 활성화를 촉진시킬 수 있을 것으로 기대된다.

ABSTRACT

In this paper, the security evaluation method about mobile web services message is suggested in the method for improving the safety an reliability about the mobile web services message. In order that the goal of this paper is accomplished, the security threat and the security vulnerability which can be occurred in the mobile web services message are defined. The evaluation method for performing the security evaluation about the mobile web services message is defined. Also, the requirements for the mobile web services message security evaluation are defined. Finally, the evaluation framework for performing the mobile web services message security evaluation is constituted, and the evaluation scenario example is suggested. By using the mobile web services message security evaluation defined in the paper, before the mobile web services is deployed, the security threats and security vulnerability can be verified. Also, the countermeasure for the security threat and security vulnerability discovered in the verification result can be prepared. Therefore, the security and reliability about the mobile web services can be improved.

키워드

모바일 웹서비스, 웹서비스 보안, 보안 위협, 보안 평가

Ⅰ. 서 론

웹서비스는 XML을 기반으로 SOAP, WSDL, UDDI 등의 표준 기술을 사용하여 서로 다른 컴퓨팅 환경에서 사용하는 모든 애플리케이션들이 직접 의사소통하고 실행될 수 있는 동적 시스템 환경을 구현해 주는 소프트웨어 컴포넌트들이다[1]. 모바일 웹서비스는 웹서비스를 모바일 환경에 적용하기 위한 서비스 기술로 모바일 환경에서 제공하는 이질적인 서비스들과 모바일 디바이스들을 통합하고, 직접 실행 가능한 동적 시스템 환경의 구성을 용이하게 할 수 있기 때문에 새롭게 주목받고 있다[2]. 모바일 웹서비스는 다양한 서비스들과 모바일 디바이스로 구성된 모바일 서비스 환경의 용이한 통합, 기존 유선 웹서비스의 재활용 및 연계를 통한 새로운 서비스의 제공 등과 같은 장점이 있다. 하지만, 관련 표준안과 기술의 미비, 구체적인 모바일 서비스 모델 및 기존 웹서비스와의 연계 방안의 부족 등으로 인해 모바일 웹서비스의 도입과 발전이 저해되고 있다. 특히, 보안 관련 표준안과 적용 가능한 보안 기술의 부족으로 인해 모바일 웹서비스가 모바일 환경에서 발생할 수 있는 수많은 보안 위협에 직접적으로 노출되어지고 있다.

본 논문에서는 모바일 웹서비스에 전달되는 메시지를 대상으로 하는 보안 위협에 대한 대응 방안을 점검하고, 모바일 웹서비스 메시지에 대한 보안 수준을 평가할 수 있는 방법들을 제시하였다. 본 논문의 구성은 다음과 같다. 2장에서는 모바일 웹서비스 보안의 개요를 간략하게 살펴보고, 3장에서 모바일 웹서비스 메시지 보안 평가에 대한 요구사항들을 정의한다. 4장에서 모바일 웹서비스 메시지 보안 평가 프레임워크를 정의하고, 이를 이용한 보안 평가 시나리오의 예를 보인다. 마지막으로 5장에서 결론을 맺는다.

II. 모바일 웹서비스 보안

1. 모바일 웹서비스 보안 기술

모바일 웹서비스 보안은 모바일 디바이스와 웹서비스 서버 사이의 통신에 대해서 전송과 애플리케이션 계층에 보안 프로토콜을 적용하여 인증, 무결성, 비밀성 등의 보안 서비스를 모바일 웹서비스를 구성요소들에 제공하는 것이다. 모바일 웹서비스 보안을 위해서는 모바일 웹서비스에 통합이 용이한 유선 웹서비스 보안 기술을 적용하는 것이 필요하다. 모바일 웹서비스 보안 기술은 새로운 보안 기술의 적용보다 이러한 기존의 웹서비스 보안 기술을 최대한 활용하는 것이 효과적이다. 이를 위해서 OMA, W3C MWI(Mobile Web Initiative) 등의 모바일 웹서비스 연구 그룹과 Nokia, Ericsson 등의 상용 업체에서는 모바일 웹서비스를 위한 전송 보안 기술로 SSL/TLS, 메시지 보안 레벨 기술로 WS-security, 애플리케이션 레벨 보안 기술로 XML-Encryption과 XML-Signature를 사용을 권고하고 있으며, 기존의 웹서비스 보안 기술을 모바일 환경에 적합하도록 수정, 확장하는 연구를 수행하고 있다 [3,4,5,6].

2. 모바일 웹서비스 보안 서비스

모바일 웹서비스에서 제공하는 보안 서비스의 목적의 하나는 서비스 거부 공격의 완화로 다음과 같은 보안 서비스를 제공한다[3].

- 인증/인가
- 비밀성/무결성
- 부인-방지/접근 제어/프라이버시
- 키 관리/보안정책

3. 모바일 웹서비스 보안 위협

모바일 웹서비스 보안 기술이 대응하기 위한 보안 위협의 유형은 다음과 같다[4].

- 부당한 콘텐츠 수정(inappropriate content modification)
- 서비스 거부(denial of service)
- 도청(eavesdropping)
- 중간자 공격(man-in-the-middle attack)
- 위장 공격(masquerade attack)
- 재전송 공격(replay attack)
- 트로이 목마 공격(trojan horse attack)

III. 모바일 웹서비스 메시지 보안 평가 요구사항

1. 모바일 웹서비스 메시지 보안 평가 개요

모바일 웹서비스 메시지 보안 평가는 모바일 웹서비스에서 예상되는 모든 보안 위협들에 대한 대응 여부와 보안 수준을 평가하는 것으로, 다음과 같은 이유로 반드시 필요하다.

- 모바일 웹서비스는 구성요소들의 형태가 다양하며, 이들의 복잡한 상호작용을 필요로 한다.
- 모바일 웹서비스 메시지는 유/무선 네트워크 모두를 통해서 전달된다. 유/무선 네트워크는 서로 다른 네트워크 환경과 보안 수준을 가지고 있다.
- 모바일 웹서비스에서 다양한 보안 서비스를 제공하기 위해서는 유선 웹서비스 보안 기술을 기반으로 보안 프로토콜 간의 상호작용이 필요하며, 유선 웹서비스 보안 기술의 수정, 확장 등을 통한 모바일 웹서비스 보안 기술들 간의 상호작용 또한 요구된다.

2. 모바일 웹서비스 메시지 보안 평가 방법

보안 평가는 목적, 대상, 적용 기준, 방법 등에 따라 평가 결과가 달라지기 때문에, 모바일 웹서비스 메시지 보안 방법에 대한 명확한 정의가 선행되어야 한다. 본 논문에서는 평가 프로그램을 이용하여 실제 시험 평가를 통한 모바일 웹서비스 메시지 보안 평가 방법을 제시한다. 평가 프로그램을 이용한 실제 시험 평가 방법은 모바일 웹서비스에서 제공하는 보안 서비스를 대상으로 실제 데이터(보안 서비스를 제공받기 위해서 필요한 데이터 값들, 예를 들어, 보안 토큰 등)를 기반으로 메시지 생성, 전달, 처리 등을 거쳐 보안 서비스를 제공받는 전체 과정을 평가하는 것으로, 모바일 웹서비스 메시지에 대한 보안 서비스가 제공되는 전체 과정을 추적할 수 있으며, 보안 위협에 대한 대응 방안 유무에 따른 처리 결과를 직접 확인할 수 있다.

3. 모바일 웹서비스 메시지 보안 평가 요구사항들

평가 프로그램을 이용하여 모바일 웹서비스 메시지 보안 평가를 실시하기 위한 최소한의 요구사항들을 다음과 같다.

- 모바일 웹서비스를 구성하는 네트워크: 모바일 웹서비스는 유/무선 네트워크의 상호작용으로 규정되며, 유/무선 네트워크 환경이 상이하기 때문에 다음과 같은 보안 평가 요구사항들을 정의한다.

-보안 평가 시 대역폭과 같은 네트워크 명세와 처리 능력의 제한을 두지 않는다.
-네트워크 노드들에 대한 접속 제한을 두지 않는다.
-네트워크 노드들에 대한 특정 요구사항들을 명세하지 않는다.
-특정 네트워크에 종속적인 웹서비스 보안 기술을 명세하지 않는다.

· 모바일 웹서비스 메시지 보안 평가 위치: 모바일 웹서비스 구성요소들에 대한 평가 위치는 다음과 같다.
-웹서비스 시스템(서버)
-웹서비스 클라이언트(모바일 디바이스)
-네트워크상의 임의 노드(회선, 라우터 등)
-모바일 웹서비스 메시지

· 모바일 웹서비스 메시지 보안 평가 제약 사항: 모바일 웹서비스 메시지 보안 평가에 대한 제약 사항은 다음과 같다.
-보안 평가는 지정된 평가 시나리오에 한정하며, T/F 만을 평가한다.
-보안 평가는 측정된 보안 수준만을 보고하며, 대응책 또는 서비스 코드에 대한 수정 방안을 권고하지 않는다.

Ⅳ. 모바일 웹서비스 메시지 보안 평가

1. 모바일 웹서비스 메시지 보안 평가 프로그램

모바일 웹서비스 메시지 보안 평가 프로그램은 그림 1, 2와 같이 보안 평가 프로그램과 보안 공격 프로그램으로 구성된다.

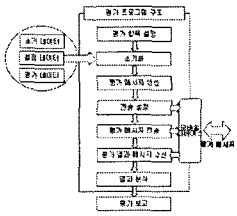

그림 5. 평가 프로그램

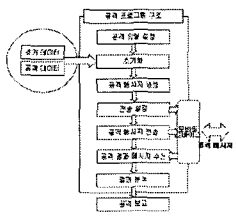

그림 6. 공격 프로그램

1.1 보안 평가 프로그램

보안 평가 프로그램의 데이터는 다음과 같다.

· 초기 데이터: 모바일 웹서비스 메시지를 생성하기 위한 기본 정보(서비스 요청을 위한 기본 정보, 송/수신 정보, 네트워크 정보 등)
· 설정 데이터: 보안 서비스 제공을 위한 보안 정보(요청 보안 서비스 유형, 대상 암호 프로토콜, 암호키, 인증서 등의 보안 토큰 등)
· 평가 데이터: 초기 데이터와 설정 데이터를 기반으로 실제 모바일 웹서비스 메시지 보안 평가 메시지를 생성하고 전송하기 위한 데이터(평가 대상 보안 위협 종류, 보안 위협에 대한 대응 방안 여부, 평가 결과 참조 값)

보안 평가 프로그램에서 수행하는 평가 프로세스는 다음과 같다.

a.초기 데이터와 설정 데이터를 입력하고, 이를 기반으로 평가 데이터를 생성한다.
b.평가 초기화를 실시하고, 평가 데이터를 기반으로 모바일 웹서비스 메시지를 생성하여 전송 어댑터로 보낸다. 전송 어댑터는 이를 보안 평가 대상 웹서비스로 전송한다.
c.보안 평가 대상 웹서비스에서 메시지를 수신하고, 이에 대한 처리를 한 후, 결과를 평가 프로그램에 전송한다.
d.평가 프로그램은 수신된 결과에 따라 모바일 웹서비스 메시지 보안 평가를 분석하고, 이의 결과를 출력한다.

1.2 보안 공격 프로그램

보안 공격 프로그램의 데이터는 다음과 같다.

· 초기 데이터: 모바일 웹서비스 메시지를 대상으로 보안 위협을 생성하고, 이를 전송하기 위한 기본 정보(보안 위협 공격을 위한 기본 정보, 송/수신 정보, 네트워크 정보 등).
· 공격 데이터: 모바일 웹서비스 메시지에 대한 실제 보안 위협을 발생시키기 위한 정보(보안 위협 유형 설정, 보안 위협의 발생 위치, 보안 위협 유형에 맞게 생성된 공격 데이터)

보안 공격 프로그램에서 수행하는 공격 프로세스는 다음과 같다.

a.모바일 웹서비스 바인딩을 위한 초기 데이터와 보안 위협을 발생시키기 위한 공격 데이터를 입력한다.
b.공격 초기화를 실시하고, 공격 데이터를 기반으로 모바일 웹서비스 메시지를 만들어 전송 어댑터로 보내고, 전송 어댑터는 이를 공격 대상 서비스로 전송한다.
c.공격 대상 서비스에서 메시지를 수신하고, 이에 대한 처리를 한 후, 결과를 공격 프로그램에 전송한다.
d.공격 프로그램은 수신된 결과에 따라 보안 위협에 대한 대응 방안 여부를 점검하고, 이를 결과로 출력한다.

2. 모바일 웹서비스 메시지 보안 평가 프레임워크

모바일 웹서비스 메시지 보안 평가 프레임워크는 1절에서 정의한 프로그램들과 모바일 웹서비스의 상호 관계와 평가 흐름, 처리 절차 및 데이터에 대한 정의이며, 그림 3과 같이 구성된다.

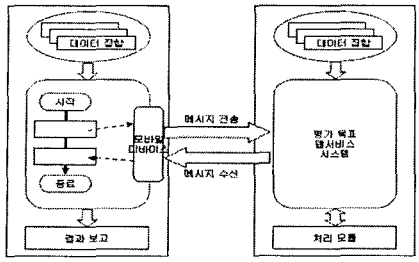

그림 7. 평가 프레임워크

3. 모바일 웹서비스 메시지 보안 평가 시나리오

모바일 웹서비스 보안 평가 시나리오는 보안 평가 항목과 보안 평가 프로세스를 정의한 것으로 보안 평가 절차이다. 본 논문에서는 다음과 같은 두 개의 시나리오를 예시한다.

- 인증과 보안 토큰 호환성 평가
- 보안 공격 대응 방안(중간자 공격을 예로)

3.1 보안 평가 시나리오 1

- 평가 목적 및 내용: 모바일 웹서비스 메시지를 통해서 전달되는 보안 토큰의 생성, 검증과 같은 처리 절차와 호환성 여부를 평가
- 평가 시나리오:

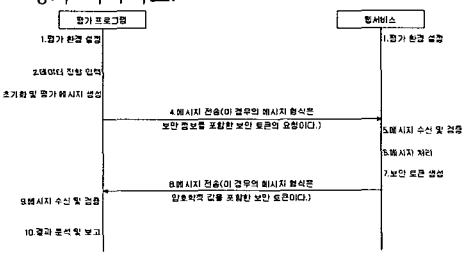

그림 4. 보안 평가 시나리오 1에 의한 평가 절차

3.2 보안 평가 시나리오 2

- 평가 목적 및 내용: 모바일 웹서비스 메시지를 대상으로 발생할 수 있는 보안 위협에 대한 대응책 여부와 처리 절차를 평가
- 평가 시나리오:

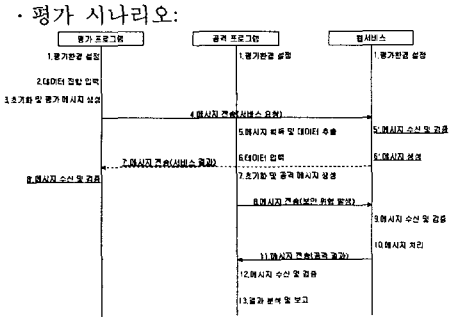

그림 5. 보안 평가 시나리오 2에 의한 평가 절차

V. 결 론

모바일 웹서비스는 시간과 장소에 구애받지 않고 웹서비스를 제공 받을 수 있다는 장점 때문에 모바일 디바이스를 이용한 인터넷의 사용이 급증하고 있으며, 다양한 모바일 웹서비스 모델들이 개발되고 있다. 모바일 웹서비스가 지금 보다 더욱 발전하기 위해서는 높은 수준의 보안성과 신뢰성이 제공되어야 한다. 모바일 웹서비스의 보안성과 신뢰성을 향상시키기 위한 방안으로 가장 대표적인 것은 높은 수준의 보안 프로토콜과 엄격한 보안 정책의 적용이다. 또한, 본 논문에서 정의한 모바일 웹서비스 메시지 보안 평가를 이용하여 사전에 보안 위협에 대한 대응책을 점검하고, 보안 취약점을 보완하며, 모바일 웹서비스 구성요소들 간에 발생할 수 있는 호환성 문제를 해결하는 것도 효과적인 방법이다.

본 논문에서는 모바일 웹서비스 보안의 간략한 개요에 대해서 설명하고, 모바일 웹서비스 메시지에 대한 보안 수준을 평가할 수 있는 방안을 제시하였다. 본 논문에서 논의된 사항은 추후 관련 표준안을 마련하고, 모바일 웹서비스 메시지 보안 평가 프로그램을 개발하는데 도움을 줄 수 있으며, 이를 통해서 모바일 웹서비스의 보안성과 신뢰성을 향상시킬 수 있는 기초를 마련할 것으로 기대된다.

참고문헌

[1] 김주한외 7명, "웹서비스 보안 기술의 표준화 및 시장 동향", 전자통신동향분석, 제20권 제1호, 2005년 2월

[2] Rich Rollman, John Schneider, "Mobile Web Services", XML 2004 Proceedings, 2004

[3] OMA Standard, "OMA Web Services Enabler(OWSER): Core Specifications-Approved Version 1.1", 28 Mar 2006

[4] OMA Standard, "OMA Web Services Enabler(OWSER): Overview-Approved Version 1.1", Open Mobile Alliance, 28 Mar 2006.

[5] OMA Standard, "Mobile Web Services Requirements-Approved Version 1.1", Open Mobile Alliance, 28 Mar 2006.

[6] NOKIA white paper, "Deploying Mobile Web Services using Liberty Alliance's Identity Web Services Framework(ID-WSF)", NOKIA, 2006