종단간 보안을 지원하는 새로운 WAP 모델

박미옥[0] 전문석[0]
숭실대학교 컴퓨터학과
mopark@kingdom.ssu.ac.kr, moon@computing.ssu.ac.kr

New WAP model for Supporting End-to-End Security

Mi-Og Park[0] Moon-Seog Jun[0]
Soongsil University Computer Science

요 약

무선통신 기술의 발달로 최근 이동 통신 사용자들은 언제, 어디서나 누구와도 통신이 가능하게 되었다. 하지만, 이동 통신은 무선채널을 사용하기 때문에 통신 당사자는 심각한 보안 위협에 노출된다. 그래서, 안전한 통신채널을 제공하기 위한 방법은 이동통신망에서 필수라 하겠다. 본 논문에서는 이러한 안전한 통신채널을 제공하기 위한 방법으로, 종단간 보안을 지원하는 새로운 WAP 모델인 WAP Agent를 제안한다. 새로운 WAP Agent는 WAP gateway를 두는 컨텐츠 제공자의 부담을 줄이면서, 안전한 보안을 제공하기 때문에 종단간 보안을 지원하는 새로운 WAP 모델로서 활용되리라 기대한다.

1. 서 론

이동통신기술의 지속적인 발달로 이동통신 사용자들은 게임, 메일전송, 은행이나 주식거래, 여행 스케줄이나 예약, 쇼핑과 같은 다양한 일을 이동통신 단말기를 사용하여 처리하고 있다. 하지만, 이동통신 가입자수의 증가와 함께 이동통신의 특성상 [1], 불법적인 서비스 이용이나 도청 또는 추적을 통한 불법적인 행위나 개인의 정보가 누출되어 악용되는 것과 같은 각종 통신 범죄 행위 등도 증가하고 있다. 본 논문에서는 현재 전 세계적으로 사용자면에서 가장 많은 수를 차지하고 있고, 공개된 표준이라는 점에서 많은 연구가 이루어지고 있는 WAP을 선택하여 이러한 이동통신상에서의 문제점을 해결하고자한다.[2]

본 논문의 구성은 2장에서는 WAP 모델과 WAP 보안에 대한 문제점을 알아보고, 3장에서는 종단간 보안을 지원하는 새로운 모델과 새로운 모델에 대한 경제성을 비교분석함으로써 WAP 게이트웨이 상에서 발생하는 보안상의 문제점을 해결한다. 마지막으로 4장에서는 향후문제를 고려한 결론을 내린다.

2. WAP

본 절에서는 기본적인 WAP 모델과 WAP에서 문제점이 되고있는 WAP Security Hole에 대해서 언급한다.

2.1 WAP 모델

WAP 모델에서는 휴대 단말기와 인터넷 서버 사이에 WAP Proxy라 불리 우는 WAP Gateway를 두도록 하고 있다. WAP Gateway의 주요 역할은 WAP 프로토콜과 인터넷 TCP/IP 프로토콜을 중간에서 변환해 주는 것이다. 다시 말하면, 모든 휴대 단말기의 인터넷 서비스 요구는 WAP Gateway를 거치도록 되어 있고, WAP Gateway는 프로토콜에 따라 요청 받은 서비스를 기존 인터넷 유선 망을 통해 다시 서비스를 요청한다. 이어서 WAP Gateway가 인터넷 서버로부터 응답을 받고 다시 서비스를 최초 요청했던 휴대 단말기에게 WAP 프로토콜로 전송함으로서 모든 과정이 이루어진다.

2.2 WAP Security Hole

WAP 게이트웨이는 웹서버 측에서 전달되는 SSL을 해독하고, 데이터를 WAP 단말기로 전달하기 전에 WTLS를 이용하여 다시 데이터를 암호화한다. 즉, WAP 서비스를 위해서는 중간의 게이트웨이를 거쳐야 하는데 WTLS로 암호화된 데이터는 WAP 게이트웨이에서 복호화된 후 SSL로 암호화되어 서버에 전달되고, 반대로 SSL로 암호화된 데이터는 게이트웨이에서 복호화된 후 WTLS로 다시 암호화되어 단말기에 전달되는 것이다. 이 과정에서 암호화되었던 원래의 데이터가 다시 복호화되므로 제 3자나 WAP 게이트웨이 관리자에 의해 보안이 침해당할 수 있다. 최악의 경우에는 WAP 게이트웨이 내부의 모든 정보를 가로챌 수 있으며[3], 결국 종단간의 보안솔루션이 필요하다. WAP 스펙에 의하면, WAP 게이트웨이가 보안 기능을 지원하는 것은 선택적인 문제로 남아있다. 그러나, 무선인터넷 상에서 무선 뱅킹(banking), 전자상거래와 같은 서비스가 활성화되기 위해서는 종단간 문제를 해결할 수 있는 기술이 준비되어야 한다[1],[4].

3. 제안한 WAP 모델

본 논문에서는 WAP 게이트웨이의 문제점을 해결하기 위해서 WAP Forum의 공식적인 표준 방법인 종단간 보안방법을 채택한다. 이러한 종단간 보안문제를 해결하기 위해서 본 논문에서는 새로운 개념의 WAP Agent를 도입한다. WAP Forum에서 제시한 종단간 보안해결책의 문제점 중의 하나는 각각의 컨텐츠 제공자가 자신의 WAP 게이트웨이를 각자 따로 설치해야하는 부담이 크다는 것이다. 그래서, 본 논문의 모델을 제시한 주요 목적은 이러한 컨텐츠 서버의 부담을 줄이면서, 종단간 보안을 지원하는 방법을 제안하기 위한 것이다.

3.1 제안한 WAP Agent 모델

WAP Forum에서 제시한 종단간 보안문제 해결방법은 컨텐츠 제공자가 각자의 WAP 게이트웨이를 안전한 장소에 따로 설치해야한다는 부담이 있었다. 본 논문에서는 이러한 컨텐츠 제공자의 부담을 줄이고 종단간의 보안문제를 해결하며, 더 높은 보안과 신뢰성을 지원하기 위해서 제안하였다.

본 논문의 모델에서는 종단간의 보안문제를 해결하고, 컨텐츠 제공자의 경제적인 부담을 줄이기 위해서 WAP Agent라는 새로운 개념을 도입한다. 그 이름에서 볼 수 있듯이, WAP

Agent는 사용자들의 일을 대신 처리해주는 기능을 수행한다. 이 WAP Agent는 단말기와 컨텐츠 제공자 사이에 위치하여, 각자 자신의 WAP 게이트웨이를 두지 않는 컨텐츠 제공자에게 WAP 게이트웨이의 역할뿐만 아니라 그 외에 필요한 부가적이고, 더 신뢰적인 역할을 수행해준다.

새롭게 제시된 WAP Agent의 기능을 살펴보면 다음과 같다.

• 기본적으로 WAP 게이트웨이에서 수행하는 기능을 지원해야 한다.

제안한 방법의 주요 목적중의 하나가 컨텐츠 제공자들이 각자 자신의 WAP 게이트웨이를 두는 부담을 줄이기위한 것이었고, WAP 게이트웨이의 역할을 대신할 수 있는 WAP Agent는 당연히 WAP 게이트웨이의 기능을 수행할 수 있어야 한다.

• WAP Agent는 다양한 사용자를 가질 수 있다.

기본적으로 본 논문에서는 WAP 게이트웨이를 두지 않는 컨텐츠 제공자들이 WAP Agent를 사용한다. 또한, WAP 게이트웨이를 두고 있는 컨텐츠 제공자가 WAP Agent에게 임의의 서비스를 요청할 수도 있다. 반면에, WAP 게이트웨이의 사용자들은 임의의 사이트를 요청하는 단말기만이 그 사용자들이었다. 결과적으로, WAP Agent의 사용자는 단말기측만 고려하더라도 아주 다양한 사용자층을 가지게 된다.

• 제 3의 인증센터와 같은 신뢰성과 보안을 제공하여야 한다.

서비스를 요청하는 여러 컨텐츠 제공자의 정보나 다른 사용자들의 정보를 누출하거나 악용해서는 안된다. 그래서, 기존의 인증센터를 사용자들이 신뢰하고, 실제로 인증센터가 그러한 신뢰성에 부합하는 역할을 하는 것처럼, 본 논문에서 제안한 WAP Agent도 이러한 신뢰성과 보안을 반드시 유지하여야 한다. 만약, WAP Agent에서 보안과 신뢰성을 유지하지 못한다면 서비스를 요청한 컨텐츠 제공자의 정보나 다른 사용자들의 정보가 누출되어 악용되는 위험성이 크기 때문이다.

• WAP Agent는 서비스의 요청이 들어오면 즉각적으로 서비스에 응하고, 투명성을 보장하여야 한다.

만약, 서비스의 요청이 delay될 경우에는 단말기 사용자에게는 훨씬 더 많은 delay를 줄 수 있고, 그에 따른 여러 가지 부정적인 영향이 있기 때문에 WAP Agent는 컨텐츠 제공자의 요구를 즉각적으로 처리하여 서비스해 줄 수 있는 메모리나 처리 능력 등을 충분히 갖추고 있어야한다.

• WAP Agent와 여러 사용자들간의 분쟁을 조절하기 위해서 기존의 인증센터를 사용한다.

WAP Agent에서 전송되고 처리되어지는 데이터들이 대부분 여러 컨텐츠 제공자들의 중요한 자료이거나 개인의 프라이버시와 관련한 민감한 정보들이기 때문에 분쟁이 발생할 경우에 이러한 분쟁을 조절하고, 더 나아가서 이러한 분쟁의 소지를 미리서 예방하기 위해서 제 3의 신뢰성이 있는 인증센터를 이용한다. 이러한 인증센터의 사용은 기존의 WAP 게이트웨이 모델에서도 지향하고 있는 부분이다.

• WAP Agent에서는 다양한 보안 등급(Class)을 지원할 수 있어야 한다.

WAP Agent는 서비스를 요청하는 측에 다양한 보안등급을 사용하여 서비스를 지원할 수 있기 때문에 기존의 WAP 게이트웨이보다 더 높은 신뢰성과 보안성을 제공할 수 있다. 이러한 문제는 기존에 다양하게 사용되는 여러 가지 사례를 연구한다면 충분히 해결될 수 있으며, 다양한 보안등급을 적용할 때는 단말기측에 적용하는 보안등급과 서비스를 요청하는 서버측에 적용하는 보안등급을 달리해야 더 효율적인 보안이 지원될 것이다. 또한, 기존에 이미 이러한 개념을 사용하고 있기 때문에, 그에 대한 구현 어려움은 없으리라 본다.

• 심각한 delay와 같은 문제의 해결방법은 Multi WAP Agents를 사용하여 해결한다.

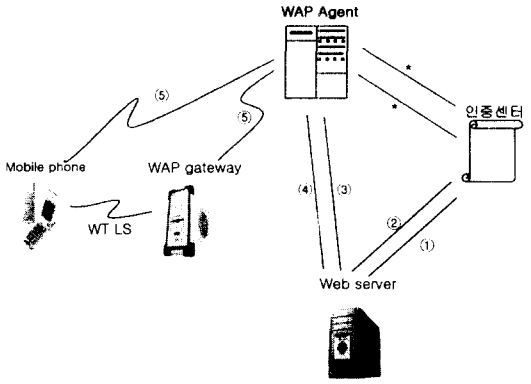
심각한 Delay와 같은 속도문제가 발생할 경우를 대비해서 모델에서는 Multi WAP Agents라는 개념을 제안한다. Multi WAP Agents라는 용어는 본 논문에서 새롭게 제안하는 용어로서, Multi WAP Agents의 역할은 여러 레벨의 WAP Agent를 두어 상호 연계하는 방식이다. 여러 WAP Agent들의 상호 연결은 신뢰성과 보안성을 기본적으로 유지해야한다. Multi WAP Agents의 확장문제는 네트워크를 확장하는 문제와 비슷하기 때문에 별다른 어려움 없이 확장가능하리라 본다.

• WAP Agent는 경제적이어야 한다.

이 모델을 제안한 주요 목적 중의 하나가 컨텐츠 제공자가 각자 자신의 WAP 게이트웨이를 따로 두는 부담을 줄이기 위해서 제안한 것이기 때문에, 컨텐츠 제공자들이 WAP Agent를 사용하는 경제적인 측면이 각자의 WAP 게이트웨이를 설치하여 사용하는 것보다 더 경제적이어야 한다. 이러한 경제성을 뒷받침하기 위해서는 WAP Agent를 사용하는 사용자들의 수가 많으면 많을수록 그 경제성이 WAP 게이트웨이를 각자 사용하는 것보다 훨씬 좋다는 것을 기본적으로 생각할 수 있고, 이에 대한 근거는 4.3절의 비교분석을 통해 알아본다. 결국, WAP Agent라는 새로운 개념을 제안한 목적이 타당하다는 것을 알 수 있다.

다음 (그림1)은 제안한 WAP Agent 모델이며, 앞에서 살펴본 WAP Agent의 기능은 다음과 같이 표현가능하다.

WAP Agent=WAP G/W + 더 높은 보안과 신뢰성



(그림 1) WAP Agent의 전송절차

①단말기로부터 임의의 사이트 요청이 들어오면, Web 서버(컨텐츠 제공자)는 그 사이트를 제공하기 위해서 먼저 인증센터에 자신의 인증서를 요청한다.

②인증센터는 인증서를 요구한 Web 서버(컨텐츠 제공자)에게 인증서를 발급한다.

③Web 서버는 자신의 인증서와 함께 단말기가 요청했던 request를 WAP Agent에게 전송한다.

④Web 서버의 요청을 받은 WAP Agent는 서비스의 결과를 단말기 측이 받을 수 있게 WTLS 형식으로 변환한다.

⑤WAP Agent에서 변환이 완성되면, WAP Agent는 WTLS 형식으로 변환시킨 데이터를 직접 단말기 측에 전송한다. 또한 WAP Agent는 Web 서버에게 Web 서버가 요청했던 서비스가 잘 처리되었다는 것을 알리는 메시지와 함께 자신의 인증서를 전송한다.

☞ WAP Agent와 인증센터사이의 별표(*)의 의미

제시한 본 모델에서는 WAP Agent의 신뢰와 보안의 수준, 그리고 이러한 환경을 제공하는데 드는 오버헤드를 고려해서, WAP Agent에 맞는 주기에 따라서 인증서를 미리 받아올 수 있다는 것을 전제로 한다.

3.2 WAP Agent의 경제성에 대한 비교 분석

본 절에서는 새로운 개념의 WAP Agent를 사용하는 모델에 대한 비교 분석을 통해 제안한 모델의 타당성을 제시한다. 비교 분석은 특별히 본 논문의 가장 중요한 부분인 경제성에 대해서만 언급한다. 그 이유는 다른 항목들은 비교분석이 대부분 앞 절에서 이미 언급되었기 때문이다.

WAP Agent의 경제성의 항목이 중요한 이유중의 하나는, WAP 게이트웨이보다 더 부가적인 기능들을 추가해야 한다는 것이다. 그리고, 부가적으로 필요로 하는 기능을 추가하기 위해서 드는 비용은 WAP Agent를 한 대를 만들었을 때 드는 비용에 모두 포함되기 때문에, 기존의 WAP 게이트웨이와의 비용을 비교하는데 좋은 기준이 될 것이다.

먼저, 전체적인 WAP Agent의 비용과 WAP 게이트웨이와의 비용관계를 알아보기 위해서 기본적으로 몇 가지의 가정을 한다. 컨텐츠 제공자를 A, B, C, D, E와 같은 대문자 알파벳으로 표기한다. 각자의 컨텐츠 제공자들이 설치해야 할 WAP 게이트웨이의 비용을 α라 하자. WAP 게이트웨이를 설치할 때 드는 비용은 환경에 따라 약간의 차이는 나겠지만, 여기서는 모두 α로 한다. 문제는 WAP Agent를 설치하는 부담이 얼마나 되는지가 문제인데, 여기서는 WAP 게이트웨이를 설치하는 비용을 α로 했을 때, 그에 대한 배수 값이 되에 WAP Agent의 비용을 설정하여 비교해 본다. 그리고, WAP Agent의 배수를 나타내는 첨자는 m으로 한다. m의 조건은 기본적으로 그 증가치를 1부터가 아니라 2부터 시작하였다. 그 이유는 한 대의 WAP Agent를 만드는 비용과 한 대의 WAP 게이트웨이를 만드는 비용을 고려해 볼 때, WAP Agent를 만드는 비용이 더 든다고 가정하기 때문이고, 이러한 가정은 WAP Agent가 WAP 게이트웨이의 기본기능에 더 부가적인 기능을 수행한다는 근거에 둔 것이다.

[수식의 의미]

컨텐츠 제공자 : A, B, C와 같은 대문자

WAP 게이트웨이에 두는 부담 : α

WAP Agent를 이용하는 부담 : m*α (m = 2, 3, ...m)

*** : 별표 세 개의 의미는 그 시점이 각자의 WAP 게이트웨이를 설치하는 부담과 동일하다는 것이고, 그 이후부터는 WAP Agent를 사용하는 것이 더 경제적이라는 것을 나타낸다.

(사례 1) 여기서는 5명의 컨텐츠 제공자를 고려해보자.

각자 5명의 컨텐츠 제공자가 각자의 WAP 게이트웨이를 설치할 경우에 드는 부담은 5개의 WAP 게이트웨이를 설치해야 하기 때문에 5α이다.

5명의 컨텐츠 제공자중 WAP Agent를 사용하는 사용자 수를 달리하면서 WAP Agent사용에 드는 부담을 계산해 보자.

①WAP Agent 사용자가 1~5명이고, WAP Agent 부담을 2α로 가정한 경우 :

2α + (5-1)α = 2α+ 4α = 6α
2α + (5-2)α = 2α+ 3α = 5α ***
2α + (5-3)α = 2α+ 2α = 4α
2α + (5-4)α = 2α+ 1α = 3α
2α + (5-5)α = 2α+ 0*α = 2α

(사례2)7명의 컨텐츠 제공자중 WAP Agent의 사용자수를 달리하면서, WAP Agent에 드는 부담을 계산해 보자. 여기서는 모든 컨텐츠 제공자가 각자 자신의 WAP 게이트웨이를 두는 부담은 7α이다.

① WAP Agent 사용자가 1~7명이고, WAP Agent 부담을 2α로 가정한 경우:

2α + (7-1)α = 2α+ 6α = 8α
2α + (7-2)α = 2α+ 5α = 7α ***
2α + (7-3)α = 2α+ 4α = 6α
2α + (7-4)α = 2α+ 3α = 5α
2α + (7-5)α = 2α+ 2α = 4α
2α + (7-6)α = 2α+ 1α = 3α
2α + (7-7)α = 2α+ 0*α = 2α

②WAP Agent 사용자가 1~7명이고, WAP Agent 부담을 3α로 가정한 경우:

3α + (7-1)α = 3α+ 6α = 9α
3α + (7-2)α = 3α+ 5α = 8α
3α + (7-3)α = 3α+ 4α = 7α ***
3α + (7-4)α = 3α+ 3α = 6α
3α + (7-5)α = 3α+ 2α = 5α
3α + (7-6)α = 3α+ 1α = 4α
3α + (7-7)α = 3α+ 0*α =3α

위의 간단한 식을 정리해보면 다음과 같다.

- WAP Agent를 사용하는데 드는 총비용
  = m*α + (WAP 게이트웨이 사용자들의 부담)
  = m*α + (n - i)α

이 식을 풀면, 다음과 같은 식을 얻을 수 있다.

- mα + nα -iα = (m + n -i)α

앞의 (사례 1)과 (사례 2)의 간단한 식에서 알 수 있는 것처럼, WAP Agent를 사용하는 사용자들이 늘수록 컨텐츠 제공자들이 각자의 WAP 게이트웨이를 두는 부담보다 훨씬 경제성이 뛰어나다는 사실을 알 수 있다. 결국, 본 고에서 제시한 WAP Agent를 사용하는 모델은 그 목적에 적합하다는 것을 살펴보았다.

4. 결론

본 논문에서 제안한 WAP Agent 모델은 종단간 보안문제를 해결하면서 WAP 게이트웨이를 설치하는데 드는 컨텐츠 제공자의 부담을 줄이기 위해서, WAP Agent라는 새로운 개념을 도입하였다. 제안한 WAP Agent는 여러 컨텐츠 제공자들의 서비스 요청을 받아 처리하기 때문에, WAP Agent를 이용하는 사용자들의 정보가 누출되거나 악용되지 않도록 보다 더 높은 신뢰성과 보안성을 제공하도록 가정되었다. 또한, 무엇보다도 WAP Agent를 도입한 목적이 타당함을 앞 절의 비교분석을 통해 알아보았다.

본 논문의 향후과제로는 더 다양한 실제적인 자료에 기본을 둔 비교분석이 필요하며, 실제로 WAP Agent를 많은 컨텐츠 제공자들이 사용할 것인가가 가장 큰 관건으로 남아있다. 이러한 향후 과제들이 해결될 때, 제시한 모델은 전자우편, 인터넷 접속, 교통, 여행, 쇼핑, 주식거래, 은행예금 서비스 등[3] 수많은 무선 인터넷 분야에 활발히 응용되어질 것이다.

[참고 문헌]

[1] http://www.baltimore.co.kr/esecurity/
[2] http://147.46.67.121/doc/
[3] http://cm.ez-i.co.kr/CP/Guide/
[4] http://www2.wips.co.kr/wap2.htm
[5] William Stallings, 'Network and Internetwork Security : Principle and Practice', IEEE Press, 1995