Mobile Security

최성곤 | ETRI 네트워크 보안구조연구팀

1. 서론

무선 네트워크의 사용자 증가와 해당 기술의 발달은 이동통신을 이용한 정보교환, 전자상거래 등과 같은 무선 네트워크를 이용한 새로운 서비스를 창출해오고 있다. 무선의 특성과 사용자의 이동에 따른 서비스 제공은 유선망에서의 보안 기술을 포함한 새로운 형태의 다양한 보안 기술을 요구하고 있다.

무선 네트워크의 사용에 따른 보안에는 크게 무선 사용에 따른 Wireless Security와 사용자의 이동성 지원을 위한 Mobile Security로 구분할 수 있을 것이다. Wireless Security는 무선 자원의 사용에 따른 위협 요소들에 대한 대응 방안에 관련된 것들이며, Mobile Security는 사용자의 이동에 따라 네트워크 내에서 처리되어야 하는 여러 가지 위협 요소들에 대한 대응 방안으로 볼 수 있다. 즉, Wireless Security는 무선 환경 그 자체에 의해 나타날 수 있는 Jamming 현상, 무선 영역에서의 Data Injecting과 수정, Man-in-the-Middle 공격 등의 다양한 위협을 인식하여, 주파수 Hopping 방식 등의 기법으로 그 위협에 대처하는 영역이라 할 수 있고, Mobile Security는 이용자의 서비스 중 위치 변경에 따른 위협, 즉 사용자의 위치 변경에 따른 Binding Update, 인증, 권한 검증 등의 위협 요소에 대해 IPSec. 등의 기법을 이용하여 그 위협으로부터 대응하는 영역이라 할 수 있다.

본 고에서는 Mobile Security를 중심으로 다양한 형태의 위협 요소와 그에 대한 대응 방안으로서의 기술적 요구사항과 동향 등을 살펴보고자 한다. 사용자의 이동성 지원은 무선 환경을 기반으로 하는 것이 대부분이다. 따라서, Wireless 환경에서의 Security가 부분적으로 포함되지 않을 수 없으며, 그 중 특히 사용자의 이동에 따라 특징지워지는 Mobile Security 부분을 집중적으로 다루고자 한다.

2. Mobile Security 기술 동향

Mobile Security를 위한 기술 표준화는 International Telecommunication Union - Telecommunication(ITU-T)의 Study Group 17과 Internet Engineering Task Force(IETF)의 Security Area에서 다루어지고 있다. 본 고에서는 ITU-T를 중심으로 기술 동향과 이슈들을 살펴본다.

ITU-T에서는 Mobile End-to-End 데이터 통신을 위한 보안 위협 요소에 대해 정의하고, 사용자와 Application Service Provider(ASP) 각각의 관점에서 요구되는 요구사항들을 정의하고 있다. 뿐만 아니라, End-to-End 관점에서 보안 기능을 확보하기 위해 어느 요소에 어떤 기술들이 적용되어야 하는 지에 대해서도 연구가 진행 중이다.

End-to-End 데이터 통신을 위한 보안 기술의 토대로는 X.msec-1의 Draft가 있고, 특정 보안 기술로써 Public Key Intrastructure를 기반으로 하는 이동 보안 시스템 설계의 기초 지침서로 X.msec-2의 Draft가 제작 중이다. 또한 보안 정책과 관련된 부분이 다음 연구 기간 동안에 진행될 예정이며 X.msec-3 Draft 문서로 정리될 예정이다.

ITU-T의 X.msec-1에서 다루고 있는 주요 내용을 정리하면 다음과 같다.

- 이동 환경에서 End-to-End 통신을 위한 모델 정의
- 이동 환경에서 End-to-End 데이터 통신에서의 특성 정리
- 이동 환경에서의 위협 요소 정리
- 이동 환경에서 End-to-End 데이터 통신을 위한 보안 요구사항 정의
- 각 요구 사항들을 고려한 보안 기능(Function) 정의
- 이동 환경에서 End-to-End 데이터 통신을 위한 보안 기법(Technology)

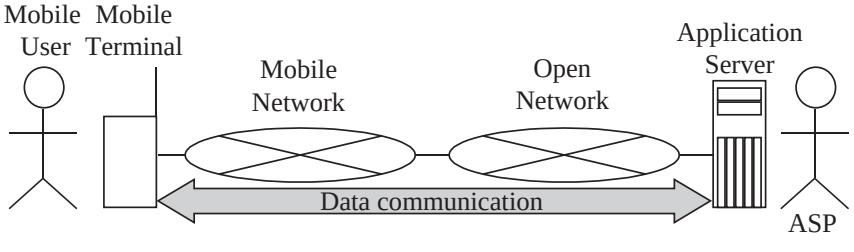
3. 보안 기술 요소

3.1 보안을 위한 네트워크 구조

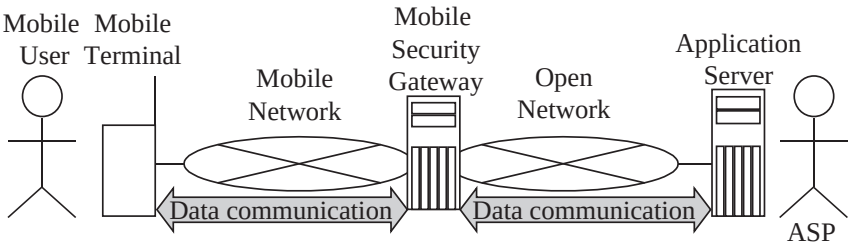
인터넷을 중심으로 한 IP 네트워크에서부터 기존의 Cellular 망에서 진화된 망에 이르기까지 보안관련 많은 연구들이 주로 운영자(ASP)의 관점에서 진행되어 오고 있다. 그러나 ASP 뿐만 아니라, 사용자의 관점에서 보안관련 항목들이 연구되어지는 것도 매우 중요한 요소가 될 수 있다.

이동 네트워크 또는 개방형 네트워크 들이 상위 계층, 즉 응용계층, 프리젠테이션, 세션 계층 등에서 다양한 형태로 구현되고 있어, 그에 해당하는 계층들에서 보안 연구들이 추가될 필요가 있다.

이러한 관점에서, ITU-T의 SG 17에서 진행되고 있는 연구 항목들을 중심으로 몇 가지 기술적 검토 사항을 알아본다. 먼저, 이동 End-to-End 데이터 통신을 위한 모델을 〈그림 1〉 및 〈그림 2〉와 같이 제시하고 있다. 〈그림 1〉은 이동 사용자와 ASP 간의 통신을 위해 Gateway 시스템을 사용하지 않는 일반적 형태를 설명하고, 〈그림 2〉는 그 사이에 Gateway 시스템이 포



〈그림 1〉 이동 사용자와 ASP 간의 데이터 통신을 위한 일반적 형태



〈그림 2〉 Gateway 시스템을 이용한 이동 사용자와 ASP 간의 데이터 통신 형태

함된 경우를 보여준다.

〈그림 1〉의 경우는 이동 사용자, 이동 단말기, 이동 네트워크, 개방 네트워크(Open network), 애플리케이션 서버 및 ASP로 구성되며 각 요소들 간의 연결에 따라 각각의 보안 관련 연구가 이루어지도록 연구를 진행하고 있으며, 〈그림 2〉의 경우는 〈그림 1〉에서 Mobile Network과 Open Network 사이에 Gateway 시스템이 추가된 것으로 두 가지의 상호 연동에 따른 보안 연구가 추가되고 있다.

3.2 이동 환경의 특성 및 보안 위협 요소들

이동 환경에서의 End-to-End 데이터 통신은 기존의 네트워크에서와는 다른 다양한 특성들을 지니고 있다. 따라서, 이동 환경에서의 보안 위협 요소는 일반적인 형태의 보안 위협 요소들뿐만 아니라, 이동 환경에서의 특성에 따른 몇 가지 위협 요소들이 더 고려되어질 필요가 있다. 이동 환경의 특성은 무선 통신을 사용한다는 특성 뿐만 아니라 이동 통신 단말기가 점차 소형화 되고 있는 특성도 있다. 이러한 관점에서 보안에 위협이 되는 요소들은 Eavesdropping, Communication Jamming, Injection and modification of data, Interruption, Unauthorized access, Repudiation 등이 있을 수 있다.

3.3 이동 환경에서의 보안 요구 사항들

이동 환경에서의 보안 요구 사항들은 크게 두 가지로 구분하여 볼 수 있다. 즉, 이동 통신 사용자 관점에서의 보안 요구 사항과 ASP 관점에서의 보안 요구 사항이 있으며, 각 항목은 다음과 같다.

- 사용자 관점에서의 보안 요구 사항
  - Identity Management
  - Data confidentiality
  - Data integrity
  - Authentication
  - Authentication
  - Access control
  - Non-repudiation
  - Anonymity
  - Privacy
  - Usability
  - Availability

- ASP 관점에서의 보안 요구 사항
  - Data confidentiality
  - Data integrity
  - Authentication
  - Access control

- Non-repudiation
- Availability

3.4 보안 관련 기능

상기한 보안 관련 요구 사항들을 만족시키기 위한 기능들은 아래와 같다.

- Encipherment : secret key와 같은 대칭 방식(symmetric encipherment)과 public key 사용과 같은 비대칭 방식(asymmetric encipherment)이 있다.
- Key exchange : encipherment 기능 수행을 위한 key 교환에 관련된 기능
- Digital signature : 데이터에 서명을 붙이는 기능과 서명된 데이터를 확인하는 기능
- Access Control : 인가된 식별자 등을 이용하여 접속 권한 부여를 결정하는 기능
- Data integrity : single 데이터 단위 및 데이터 stream 단위의 두 가지 측면이 있으며 서로 다른 기법이 적용된다.
- Authentication exchange : 상대측의 인증을 위해 적용되어질 수 있으며 패스워드와 같은 정보의 사용, 암호 기법 등이 사용될 수 있다.
- Notarization : 두 개 이상의 개체들간에 통신이 있을 때 제 3 자에 의해 공증 받는 형태의 기능

상기한 기능들을 상기한 요구사항들과 관련 지어보면 아래 〈표〉와 같다.

〈표〉 보안 요구사항과 기능과의 연관성

기능 / 요구사항	Encipherment	Key exchange	Digital signature	Access control	Data integrity	Authentication exchange	Notarization
Identity management	X	X	X			X	
Communication data confidentiality	X	X		X		X	
Stored data confidentiality	X			X			
Communication data integrity	X	X	X	X	X	X	
Stored data integrity	X		X	X	X		
Entity authentication	X		X			X	
Message authentication	X	X	X		X	X	
Access control				X		X	
Non-repudiation			X			X	X
Anonymity	X						
Usability				X			
Privacy	X			X		X	
Availability				X		X	

4. 향후 추진 방향 및 결론

지금까지 ITU-T를 중심으로 한 이동 환경에서의 보안 관련 기술 동향과 이슈 등을 살펴보았다. ITU-T에서는 기존의 보안 관련 기술 검토를 거쳐 사용자 관점에서의 보안 요구사항과 서비스 제공자 중심의 요구사항들을 각각 검토하여 이에 대응할 수 있는 기능들을 정리해 나가고 있다. 이러한 요구 사항들은 기존의 유선 망에서의 요구사항들을 포함하여 무선 환경에서 요구되는 특정 요구 사항들을 추가하고 있다.

이러한 이동 환경에서의 보안 표준화 작업은 기초 단계에서부터 조심스러우나 매우 활발한 진행이 이루어짐을 볼 수 있다. ITU-T SG 17에서는 다음 토의 안건들 중의 하나로 이동 환경에서의 보안 정책(Policy) 분야를 선택하고 있다. 이는 상기한 내용의 구성(framework)과 요구 사항들을 바탕으로 진행될 예정이며 네트워크 객체(Entity)와 서비스 제공자 사이에서 보안 정책 기능 수행을 위한 세부 항목들을 정의해 나갈 것이다. 또한, IETF의 Working group 'mobike'에서는 IKEv2의 address update관련 문서를 시초로하여 IPsec 적용을 위한 IP overhead 절감 방안, Address update를 위한 Key 확장 방안 등이 논의될 예정이다.

[참고문헌]

[1] Tadashi KAJI, et, al, "TD2370 : Final draft of X.msec-1 and X.msec-2," ITU-T, SG 17, Mar.,2004.

[2] Jianyong Chen, "TD2378 : Baseline document of X.msec-3 for further discussion," ITU-T, SG 17, Mar.,2004.

[3] Merritt Maxim & David Pollino, "Wireless Security," RSA Press, 2002.