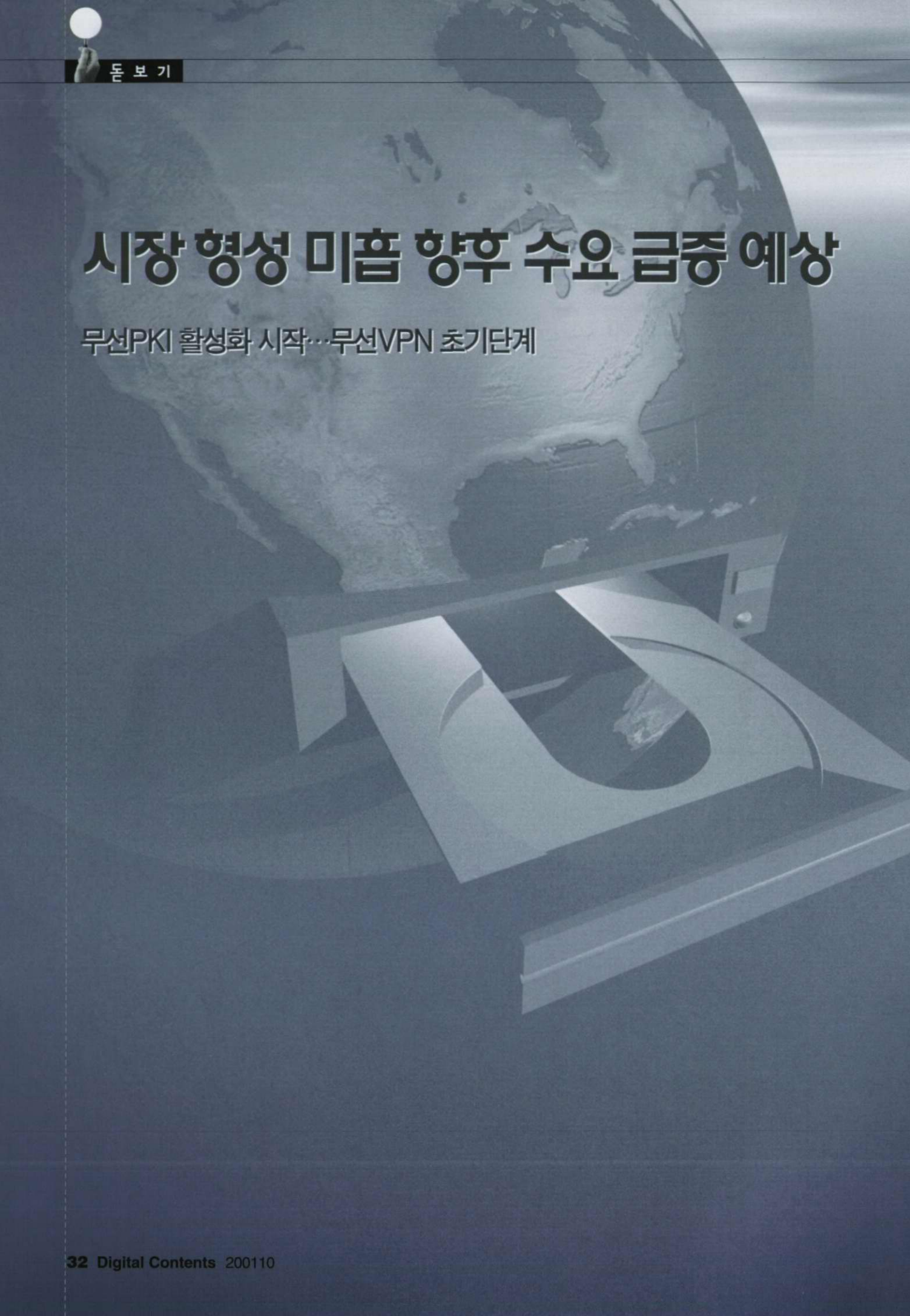
시장 형성 미흡 향후 수요 급증 예상

무선PKI 활성화 시작…무선VPN 초기단계



무선 인터넷 서비스의 수요는 국내외적으로 크게 증가하고 있으며 2003년경 전 세계 무선 인터넷 사용인구가 6억 명에 이를 것이라는 전망이 나오고 있다. 이러한 급속한 발전에 비해 무선 인터넷 관련 기술은 아직 초기 시작 단계이다.

무선 인터넷 서비스 제공을 위한 프로토콜을 이동통신관련 업체들이 주축이 되어 개발하고 있으나 아직 표준화가 확립되지 않은 상태이다.

또한 무선 인터넷을 이용한 뱅킹 서비스, 주식 거래, 온라인 쇼핑 등의 전자상거래 서비스를 원활히 제공하기 위해서는 유선인터넷과 마찬가지로 보안 문제가 해결되어야 하나 아직 국제적인 표준화가 진행중에 있는 실정이다.

국내 이동통신가입자의 증가와 함께 무선 인터넷에 대한 수요 또한 증가하고 있으며 이에 따른 보안의 필요성이 대두하고 있다.

이에 따라 한국정보보호센터에서는 무선 인터넷 PKI(Public Key Infrastructure)를 개발하고 있으며 향후 국내 무선 인터넷 PKI 체계 구축을 추진하고 있다.

국내 동향

현재 국내에서 무선 보안과 관련해서 개발중인 업체는 그리 많지는 않은 실정이다.

이는 아직 무선 보안시장이 활성화되어 있지 않은 현실과 전반적인 경기 침체가 그 원인으로 지적되고 있다.

그러나 몇몇 업체에 의해 무선 PKI와 모바일 VPN 분야가 개발되어 졌으며, 무선 백신 분야도 현재 개발 중에 있다.

따라서 무선인터넷의 활성화가 이루어지는 시점에 무선 보안 시장도 형성될 것으로 업계에서는 전망하고 있다.

무선 인터넷 활성화 먼저 이뤄져야

또한 국내 이동통신서비스는 1990년대 중반을 기점으로 크게 증가 2000년말 현재 약 2천800만명의 가입자를 보유하고 있으며 약 100만명 이상이 무선 인터넷 서비스를 이용하고 있다.

국내 무선 인터넷 접속 기술은 크게 WAP계열과 ME계열로 나누어 볼 수 있다.

SK텔레콤, 신세기이동통신, LG텔레콤이 WAP 서비스를

Mobile-VPN | 전문가 기고

Mobile-VPN의 개념과 WINGS-MV 소개

엠아이시큐리티 개발2팀 팀장 박왕석

무선인터넷의 보안이라 하면 보안이라는 측면이 개발자 측면에서 보면 기술적으로 어느 부위에서 보안 서비스를 제공하느냐에 따라 상이하게 보여진다. 혹자들은 유선의 시스템을 그냥 무선의 환경에 옮겨 놓으면 되리라 생각하는데 전혀 그렇지가 않다. OS 환경을 참조하더라도 유선의 경우에는 서버 환경에서는 UNIX, Windows NT, Linux로 대변되고 클라이언트에서는 Windows 환경으로 사실상의 표준이 이루어져 있다. 그러나 무선의 환경은 전혀 그렇지 못하다. 핸드폰의 환경은 모든 제조사 별로 별도의 S/W를 가지고 있고 또 그것이 그 회사의 기술력으로 인식되고 있기 때문에 표준이라는 것이 전혀 존재할 수도 없고 PDA의 경우에도 WinCE Pocket PC, WinCE Hand Held PC, Palm, Linux, Cellvic 등 너무나 많은 시스템들이 존재한다. 그래서 무선인터넷의 보안은 그 이론적인 기술도 무선인터넷 보안 솔루션을 개발하는데 중요한 요소이지만 그 이론적인 기술을 무선의 환경에 적용하는 기술이 아주 중요하게 작용한다. 즉, 무선인터넷 보안 시스템 개발자들은 유선상의 보안 시스템 개발자들 보다 아래의 사항들에 대한 문제를 풀어야 한다는 추가적인 제약이 있기 때문에 그 개발시간이나 알고 있어야 하는 기술적인 환경들이 더욱 복잡하다.

〈무선인터넷 보안 시스템 개발자들이 가지는 기술적인 환경〉

▲유선 인터넷 보안기술(프로토콜, 알고리즘 등의 표준기술)

▲무선 인터넷 프로토콜(WAP, ME, I-Mode 등)

▲무선 단말기 OS(WinCE, Palm 등)

▲무선 단말기 CPU(Strong ARM, MIPS, SH3 등)

▲암호화 알고리즘 최적화 기술(무선 단말기는 PC에 약 1/5 정도의 컴퓨팅 파워)

▲입력 정보의 최소화 기술(무선 단말기에 정보 입력은 PC에 비해 많이 어렵다.)

▲유무선 통합기술(기업의 유선 환경을 무시한 무선 환경에서만 사용되어 질 수 있는 무선 인터넷 보안 제품은 절름발이 제품이다.)

이러한 무선인터넷 보안 환경 속에서 Mobile-VPN은 어떻게 이루어져있는가? M-VPN의 경우도 유선의 VPN과 같이 현재 VPN 국제 표

제공하고 있으며, KTF가 ME서비스를 제공하고 있다.

그러나, 현재 WAP계열 서비스의 경우 WTLS를 아직 적용하고 있지 않으며 ME의 경우 국내 서비스를 위하여 SSL을 개발하였으나 아직 보편적으로 이용되고 있지 않다.

현재 제품을 개발하고 있는 업체는 드림시큐리티가 Trust-M이라는 WTLS를 개발했으며 이어 CA, PKI 제품군을 개발했다.

이니텍은 현재 WTLS를 구현 중이며 소프트포럼은 MS의 ME용 SSL을 개발하여 국내 ME제품에 적용했다.

엠아이시큐리티도 무선 인터넷 PKI 제품을 개발했으며, 현재 모바일 VPN 제품을 개발 완료 단계에 있다.

이외 인젠, 넷시큐어, 시큐아이닷컴에서도 무선 인터넷 관련 보안 제품을 연구 개발 중에 있으며, 안철수연구소와 AI시큐리티가 함께 무선 백신 제품을 개발 중에 있다.

▲ 무선 PKI

현재 내년중에 실시할 예정인 무선인증 서비스용 11개 무선 공개키기반구조(PKI) 기술규격안이 마련됐으며, 또한 최상위 공인인증기관(루트 CA) 서버시스템 구축도 완료된 상태이다.

따라서 SK텔레콤 등 이동통신 3사에 이어 4개 공인인증기관의 무선PKI 인증시스템 구축작업이 급류를 탈 것으로 예상된다.

또 무선인증 서비스 부문의 공인인증기관 지정도 곧 이뤄질 전망이다.

무선PKI 인증 시스템 급류 탈 듯

한국정보보호진흥원은 지난 8월 29일 무선인증서 관리프로토콜, 무선 응용계층 보안프로토콜, 무선 전자서명 인증서 프로파일, WTLS(Wireless Transport Layer Security)인증서 프로파일, 무선 전자서명 인증서 OID(Object IDentifier) 등 11개 무선PKI 기술규격을 마련한 데 이어 인증서비스 관련업체와의 협의를 거쳐 이들 규격을 연내에 표준안으로 확정할 방침이라고 밝혔다.

KISA는 또 최상위 공인인증기관 서버시스템 구축완료와 함께 공인인증기관 실질심사에 필요한 평가기준 및 지침도 완성단계에 이르렀다고 보고 평가지침 후 공인인증기관의 실질심사 요청이 있으면 엄정한 실질심사를 통해 공인인증기관을 지정할 방침이다.

〈 표-1 〉 무선 PKI 인증서비스 구축현황

이동통신업체	시스템구축업체	시스템방식	암호알고리듬	내용
SK텔레콤	시큐어소프트	WAP	ECC	시스템 구축 및 시범서비스 완료
KTF	드림시큐리티	ME	ECC	시스템 구축 완료
LG텔레콤	케이사인	WAP	ECC	시스템 구축 완료

KISA 이재일 인증관리팀장은 "11개 무선PKI 기술규격과 최상위 공인인증기관 서버시스템 구축이 완료됨에 따라 이제는 공인인증기관 지정 실질심사를 위한 정보통신부의 지령만 남았다"며 "이동통신 3사의 무선인증 서비스 시행에 차질이 없도록 했다"고 말했다.

한편 공인인증기관들도 WPKI 기술규격안 마련과 루트CA 서버시스템 구축과 때를 맞춰 무선PKI시스템 구축에 박차를 가하고 있다.

한국정보인증의 경우 KTF · SK텔레콤 · LG텔레콤 · 케이사인 등의 시스템 구축을 조만간 완료할 예정이다.

또한 한국정보인증은 이들 시스템의 구축과 함께 곧바로 무선인증 서비스 부문 공인인증기관 심사를 KISA에 요청할 계획이다.

한국증권전산도 PDA 등 무선 인터넷기반 증권거래시장을 겨냥해 왑(WAP) 및 MME(Microsoft Mobile Explorer) 지원

이밖에 금융결제원은 무선PKI 시스템 구축을 위한 업체 선정 방안을 마련중이다(표-1 참조).

▲무선VPN

무선 VPN 시장은 아직 말 그대로 미 개척 분야이나 다름이 없다 현재 국내에서는 엠아이시큐리티 혼자서 고분분투하면서 제품 개발에 박차를 가하고 있다.

MI 시큐리티 혼자 고분분투

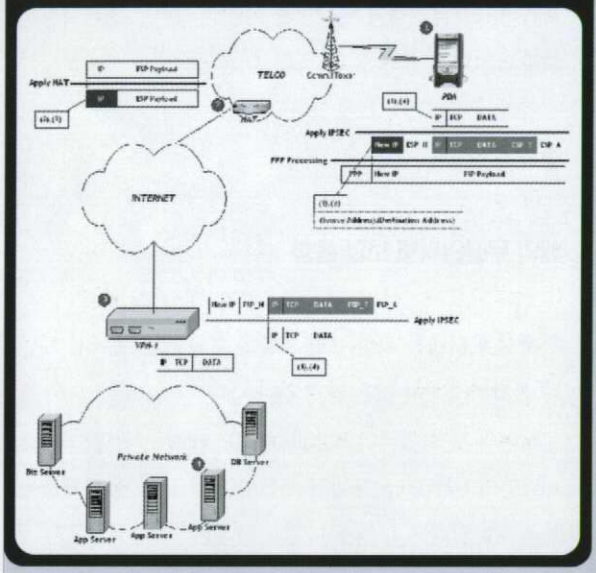
엠아이시큐리티는 최근 개발한 무선 가상사설망(VPN) 클라이언트 평가판(WINGS-MV)을 최근 홈페이지를 통해 공개하기로 했다고 밝혔다.

이 평가판은 시스코 · 노텔 · 체크포인트 · 시만텍 등 유선 VPN 그룹웨어 및 리눅스용 VPN 그룹웨어(프리스완) 등과 연동해서 사용할 수 있다.

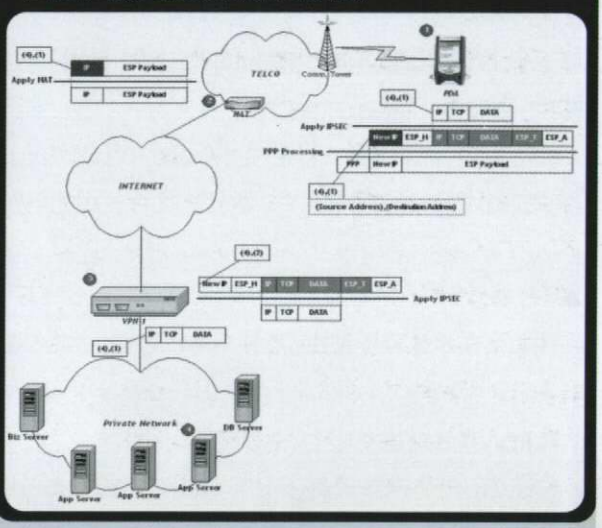
또 이동통신 사업자가 제공하는 IS95C, IMT2000 망에서도 사용할 수 있다.

엠아이시큐리티 서동형 팀장은 "WINGS-MV는 제품이 출시된지 2주일 만에 제조사, 증권사, 생보사 등 많은 사업분야에서

〈 그림1 〉 패킷 흐름도 (사용자에서 서버로)



〈 그림1 〉 패킷 흐름도 (서버에서 사용자로)



준인 IPSec을 수용한다. 즉 모든 VPN 시스템의 동작은 유선상의 VPN과 같이 동작한다는 것이다. 여기에서는 IPsec에 대한 이해를 전제로 하여 구체적으로 PDA 단말기에서 VPN G/W를 거쳐 Application Server 이르는 동안에 이루어지는 패킷 교환에 대해 간략히 알아보고자 한다. 사용자가 PDA를 이용해 이동통신 사업자의 무선인터넷망에 로그인을 하게 되면, PDA에는 이동통신사업자가 할당해주는 사설IP가 할당되어진다. 그리고, 이와 함께 NAT 장비에는 사설 IP에 해당하는 공인 IP가 할당되어 PDA를 통한 인터넷 접속이 가능하다. 또한, 사설 IP와 공인 IP간에 1:1 매칭을 시켜주기 때문에 외부에서도 PDA에 접속할 수 있다.

(1)사용자는 자신이 접속하고자 하는 VPN Gateway와 WINGS-MV 클라이언트 프로그램을 이용하여 상호인증 및 보안 채널을 형성한다.

(2)보안채널이 형성된 후, 사용자가 VPN Gateway 내부의 Private Network에 접속을 시도하면, PDA에 설치되어 있는 VPN 모듈이 IP 패킷을 암호화하고 ESP Packet을 만들고, 새로운 IP Header를 덧붙여 새로운 IP 패킷을 생성한 후, 이를 PPP모듈로 전달해준다. PPP 모듈은 전달받은 IP 패킷을 PPP Header로 감싼 후, 이동통신 사업자의 PPP Server에게 전달한다.

(3)PPP Server는 수신한 PPP 패킷에서 PPP Header를 제거한 후, IP Packet을 NAT 장비로 전달하게 된다.

(4)NAT 장비는 수신한 IP Packet의 Source Address를 공인 IP로 바꾸어준 후, 이를 VPN Gateway로 전달한다.

(5)VPN Gateway는 수신한 IP Packet으로부터 ESP Packet을 추출한 후, 이를 복호화하여 원본 패킷을 복원한 후 내부 네트워크으로 전달해준다. (1)서버가 사용자에게 데이터를 보내면, VPN Gateway는 IP Packet을 사용자와 협의한 IPSEC SA를 이용해 암호화하여 ESP Packet을 구성한다. 그리고, 새로운 IP Header를 덧붙여 IP Packet을 만든 후, 이를 인터넷망을 통해 사용자에게 전송한다. (2)NAT 장비는 사용자에게 전달되는 IP 패킷의 Destination Address를 사용자의 PDA에 할당되어진 사설 IP 주소로 변환한 후, 내부 무선 인터넷망을 통해 사용자 PDA로 전달해준다. (3)사용자는 수신한 IP 패킷으로부터 ESP 패킷을 추출하고, VPN Gateway와 협의한 IPSEC SA를 이용해 복호화하여 원본 패킷을 복원한다. 그런 후, 이를 상위 레이어로 전달해준다. 이런 식으로 암호화된 패킷 교환을 통해 end to end 보안을 이루어 낼 수 있는 것이다. 엠아이시큐리티의 WING-MV는 이러한 방식을 거쳐 구현 되었을 뿐 아니라 경제적으로도 바로 현장에서 쓰일 수 있도록 몇 가지 특징을 갖고 있다. (1) 표준화된 기술 = Ipsec 표준 및 암호화 알고리즘의 표준 준수로 표준을 따르는 어떤 VPN G/W와의 연동 가능 (2) 기존의 G/W와의 연동성 = 특히 CISCO, Checkpoint, Nortel, Symantec 등 가장 범용적인 VPN G/W와 호환되며 따라서 기존의 유선 VPN 환경에 별다른 추가 없이 단지 PDA 단말기에 S/W Module 탑재만으로 바로 VPN을 이용한 보안 형성이 가능. (3) 다양한 Analyzing Tool 제공 = PDA 단말기 내에서 Ipsec Log 및 IKE Log를 보고 분석이 가능하여 어떠한 돌발 변수에도 대응이 가능함. (4) 편리한 사용 = Quick Logon 등 많은 편리 기능을 구현하여 user 지향적인 사용환경 구현.

관심을 보이고 있고 그 활용성을 인정받아 현재 2개 기관은 계약 단계에 있다"며 "무선인터넷의 활성화와 무선인터넷을 이용한 응용시스템에 보안 서비스를 활성화하기 위해 클라이언트 평가버전을 공개하게 됐다"고 설명했다.

또한 "현재 무선 VPN 시장은 열리지 않았지만, 현재 앞으로의 수요를 예측하면 폭발적인 수요가 있을 것"이라고 전망했다.

▲무선 백신

현재 무선 백신 제품을 개발중인 업체는 안철수연구소와 IA시큐리티가 공동으로 제품 개발중에 있다. 또한 백신 보안업체들의 PDA 백신 제품 개발이 러쉬를 이루고 있다.

지난 7월 안철수연구소는 무선인터넷상의 바이러스 창궐을 예방하기 위해 SK텔레콤과 공동으로 개발에 나선다고 밝혔다.

안연구소, AI시큐리티와 공동 개발

관련업계에 따르면 SK텔레콤과 안철수연구소의 자회사인 IA시큐리티는 무선인터넷용 보안 솔루션 개발을 마치고 SK텔레콤 시스템에 맞도록 최적화하는 단계에 돌입한 것으로 알려졌다. 무선인터넷 앤티바이러스 솔루션 개발은 IA시큐리티가 안철수연구소의 엔진 및 각종 노하우와 SK텔레콤 무선환경 기술의 도움을 받아 추진중이다.

양사 관계자는 PDA 앤티바이러스 솔루션 개발은 거의 완료된 상태며 시험을 거쳐 올해 안에 구동이 가능할 것으로 내다봤다.

안연구소의 한 관계자는 "무선인터넷 시장이 아직 크지 않아 바이러스가 널리 유포되지 않았지만 관련 시장이 급팽창할 것으로 보인다"며 "이에 대비하기 위해 무선인터넷 백신 개발에 나서게 됐다"고 말했다.

또한 현재 PDA용 백신 개발은 트렌드마이크로, 시만텍 등 외산 업체들이 앞서나가고 있는 상태이다.

가장 먼저 PDA용 백신을 선보인 업체는 한국트렌드마이크로이며, 이 회사는 지난달 중순부터 자사 홈페이지를 통해 PDA용 백신인 PC실린와이어리스를 무료 배포하고 있다.

이 백신인 팜OS, 윈CE, 심비안 등을 지원하며 전자우편에 첨부돼 있는 바이러스까지 검색할 수 있다.

시만텍코리아는 최근 본사에서 출시한 PDA용 백신의 한글버전을 지난 5월경 국내에 출시했다.

시만텍의 PDA용 백신은 팜OS 전용으로 바이러스에 감염되기 전에 실시간으로 바이러스를 유무를 확인해 사용자에게 경고하는 자동보호기능과 인터넷을 이용한 라이브 업데이트 기능을 갖추고 있다.

특히 용량이 50KB에 불과해 저장 공간이 적은 PDA에 부담을 주지 않는다.

해외 무선인터넷 보안 동향

무선 인터넷을 위한 보안 기술은 현재 많은 곳에서 개발 중이나 실제 제품화된 것은 많지 않다.

국외의 경우 영국의 Baltimore Telepathy, 핀란드의 Sonera, 캐나다의 Certicom 등에서 무선 인터넷 PKI 관련 제품을 개발 판매하고 있다.

아직 개발 완료는 그리 많지 않아

무선 인터넷을 위한 인증서는 아직 그 규격이 완전히 정립되지 못하였으나 현재 WTLS 서비스 제공을 위하여 VeriSign과 Entrust.net에서 WAP 서버를 위한 인증서를 판매하고 있다. 이 인증서들은 인증서 상태검증 서비스를 제공하고 있지 않으며 특히 VeriSign의 경우 단말의 CRL확인 대신 CRL 갱신 주기 보다 짧은 25시간용 인증서를 사용으로 대체하고 있다.

무선 인터넷에 대한 관심이 고조되면서 많은 업체들이 무선 인터넷을 위한 보안 제품 개발을 하고 있다.

그러나 현재 무선 인터넷 PKI의 모델, 규격에 대한 정의가 완전히 내려지지 않았으며 무선 인터넷을 위한 인증서 및 관련 기술에 대한 표준이 없는 실정이다.

무선PKI | 전문가 기고

WPKI(Wireless Public Key Infrastructure) 소개

드림시큐리티 무선기술팀장 최준호

무선인터넷 서비스의 수요는 국내외적으로 크게 증가 하고 있으며 2003년경 전 세계 무선 인터넷 사용자가 6억명을 넘을 것이라는 예측이 나오고 있다.

이러한 급속한 확산 추세에도 불구하고 무선인터넷 관련 기술은 초보단계의 수준을 벗어나지 못하고 있으며 보안기술 또한 국소적으로 기술 개발이 이루어지고 있는 상태이다.

무선 보안 기술 개발의 어려움은 기존 인터넷 환경에 비해 무선 단말기를 이용하는 경우 표시 할 수 있는 화면이 작은 데다 네트웍 대역폭의 한계,느린 CPU,제한된 기억장치, 밧데리 소모량 등 기존 환경에 비해 매우 열악함에 기인한다.

이러한 열악한 환경에도 불구하고 사용자는 휴대성, 즉시성, 간편성 등 무선의 장점 때문에 무선을 통한 거래, 정보 획득, 커뮤니케이션 등을 원하고 있다.

이러한 트랜젝션의 발생은 개방형 시스템을 지향하고 있는 현실을 볼 때 기밀성, 무결성, 인증(권한), 전자서명을 통한 부인방지 등을 추구 할 수 있는 인프라가 꼭 필요하며 이러한 필요성을 충족시키는 인프라가 WPKI다.

여기서는 지면 상의 이유로 PKI기술에 대한 세부적인 사항을 필력하기 보다는 WPKI가 가지고 있는 장점 및 특징 위주로 기술하겠다.

WPKI의 특징은 크게 다음과 같이 4가지로 요약 할 수 있다.

1. ECC(타원곡선 알고리즘)의 상용화이다.

유선에서 표준으로 사용하고 있는 RSA 알고리즘을 이용하여 무선 단말기에서 키쌍을 생성할 때 수분 이상이 소요되며 전자 서명을 할 때도 수 십초 이상이 소요된다.

이에 반해 같은 비도를 가지고 있는 ECC알고리즘을 사용 할 경우 키 쌍 생성 및 전자 서명은 2 ~3 초 이내에 이루어진다.

2. Short - Lived - Certificate의 등장이다.

PKI의 근간인 인증서를 사용 할 경우 인증서 검증은 필수적이며 인증서 검증 메커니즘은 인증서 자체에 대한 검증, 인증서의 상태 확인,인증서 체인 검증 등이 이루어 져야 한다.

기존 PKI에서는 인증서 상태 확인을 할 수 있는 방안은 CRL을 이용하여 하고 있으나 CRL의 발급 주기 및 획득 주기를 고려 할 경우 CRL이 현재의 정확한 인증서의 상태를 나타내기는 어려우며 또한 그러한 시간의 차이는 어느 정도 인정을 하고 있다.

이러한 사상을 기초로 인증서의 유효기간을 24시간 또는 48시간으로 한정함으로써 인증서의 상태검증 과정을 생략하자는 것이 Short - Lived - Certificate이다.

3. 인증서의 저장 및 전달 방법이다.

현재 유선에서는 인증서 전체를 저장하고 또한 인증서 전체를 송,수신 하는 것에 반하여 WPKI에서는 인증서를 획득 할 수 있는 위치(인증서 URL)만을 저장하고 송,수신 할 수 있다.

이러한 방법을 사용 할 경우 무선단말기에서도 많은 인증서를 저장 할 수 있을 뿐만 아니라 인증서 전달에 있어 통신 비용의 절감의 효과를 기대 할 수 있다.

4. 유선과는 다른 인코딩 방법이다.

유선 PKI에서는 BER 또는 DER을 사용하여 정보를 인코딩 하였으나 무선 단말기에서 BER 또는 DER을 전적으로 수용하기는 무리임으로 XDR을 이용하여 정보를 인코딩한다.

위에서 기술 한 것 이외에도 전자 서명 메시지 포멧 이나 Device Certificate 등 무선 환경에 적합한 사항들이 있다.

일각에서는 WPKI 등장은 무선 단말기의 열악한 환경에서 기인 한 만큼 무선 단말기의 환경이 좋아지면 자연 도태 될 것이라는 주장을 내 놓고 있다.

하지만 WPKI 규격을 조금만 더 자세히 들여 다 보면 WPKI 규격 자체는 무선에서만 사용 할 수 있게 만든 규격 이라기 보다는 기존 PKI규격을 수용하면서 무선 환경에 맞는 규격으로 확장한 것임을 알 수 있다.

이러한 연유로 향후 WPKI는 PKI의 한 층 더 발전 한 모습이라 말 할 수 있다.