모바일 DRM, M-Commerce 확대의 중심에 서다!

시스템 구축으로 돈벌고 보안확보로 돈 새나가는 것 막아주고

연 재 순 서

1. 모바일비즈니스와 콘텐츠 (이번호)
2. 모바일 DRM의 필요성
3. 모바일 DRM 특성
4. 모바일 DRM 구축현황

김진영 비즈니스 컬럼리스트
(digilite@korea.com)

지금까지 보안이라고 하면 주된 논의 대상은 유선에 집중돼 왔다. 유선시장이 먼저 도래한 탓이겠지만 이제 점차 부각되고 있는 무선시장에서도 보안에 대한 관심 증대와 실제 구축작업이 진행 중에 있다. 실제로 무선 환경에서의 보안은 유선 환경보다 상당히 취약한 것으로 평가되고 있다.

모바일 보안의 비즈니스적 접근

지난해 한 보안 관련 컨퍼런스에서 불법적으로 무선 데이터를 캡처하는 방법을 들은 바 있다. 혹시 일전 언론에서 도청의혹과 관련해 소개됐던 CDMA용 청취기기라는 것을 들은 사람들은 상당한 장치를 생각했을 듯하다. 하지만 데이터 캡처를 위해 필요한 것은 안테나 역할을 하는 프링글스 감자칩 케이스와 노트북, 전선 몇 가닥이면 끝이다. 맘만 먹으면 누구나 쉽게 도청을 할 수 있다는 얘기다.

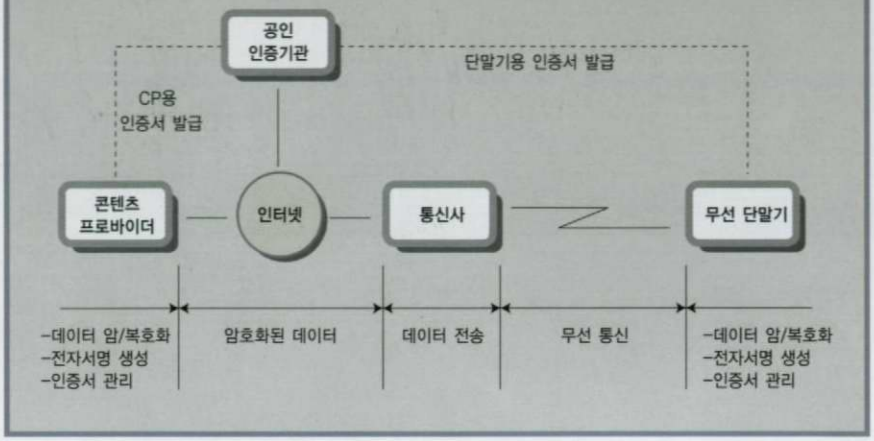
사실 무선데이터를 무선 형태로만 감청 · 획득할 수 있는 것은 아니다. 무선인터넷의 절반은 유선환경이기 때문이다. 이 때문에 CDMA 감청이 가능한가 아닌가에 대한 논란도 계속 되는지 모른다.

우선 무선 환경의 보안은 유선과 비슷한 양상으로 W-PKI와 모바일VPN 등 양 갈래로 진행되고 있다. 물론 필자의 연재 목적이 W-PKI나 모바일VPN 그 자체에 있지는 않다. 다만 모바일 보안의 새로운 카테고리로 자리 매김할 모바일 DRM(Digital Rights Management)을 상세히 설명함에 있어 보안 솔루션의 차이와 그 속에 담긴 비즈니스적/기술적 암시나 중요 포인트를 우선 확인하고자 한다. 〈디지털콘텐츠〉 독자여러분들께서는 이 점을 참고해 일독해 주실 것을 부탁드린다. 또한 단순한 기술 소개보다는 좀 더 가치 판단 위주의 내용을 강조하고자 한다.

W-PKI, 기술적 한계 남아

PKI(공개키 기반구조)의 사용은 이미 국내에선 일반화돼 있다. 인터넷 뱅킹이나 온라인 주식거래에서 광범위하게 사용되고 있을 뿐 아니라 개별 기업 차원에서도 B2B 거래나 내부 거래를 위해 적용되고 있다. PKI 적용의 목적은 보안 요구사항인 기밀성(정당한 권리를 가진 사람이 데이터를 사용함), 무결성(메시지의 위/변조 차단, 불법 재사용 차단), 인증(신원 확인), 부인봉쇄

〈그림1〉 W-PKI 구조도



(송 · 수신자간의 분쟁 해결) 등이다. W-PKI라고 해서 이와 다를 바는 없다.

PKI는 다음과 같은 구성 요소를 가진다.

- 공인 인증서를 발급하고 확인하는 인증기관(CA)
- 디지털 인증서 발급을 위해 사용자가 등록절차를 제공하는 등록기관(RA)/무선 환경일 경우 RA + CA = 이동통신사가 될 수도 있다.
- 공개키를 가지는 디지털 인증서
- 인증서관리 시스템

다만 무선 환경과 사용자 단말기의 차이로 유선 PKI와 무선 PKI에 차이점이 발생한다. 기본적으로 PKI는 인증서를 근간으로 작동하게 된다. 즉 사용자 PC에 저장돼 있는 인증서의 유효기간을 정기적으로 확인하게 되는데 이는 상당한 부하를 가져온다. PC에서는 큰 무리가 없으나 메모리나 CPU 측면에서 현재의 무선 단말기는 이를 감당하기 어려운 것이 사실이다. 따라서 확인보다는 유효기간을 단축해 제공하는 방법을 고려하기도 하는데 이를 SLC(Short Lived Certificate)라고 한다. 물론 이럴 경우에는 인증서 발급 횟수 자체가 많아짐으로 해서 인증기관의 부하가 커지게 되는 부작용은 있다.

유선 PKI와 무선 PKI의 또 하나의 차이점은 암호화 알고리즘이다. 유선 PKI에서는 암호화 알고리즘으로 대부분 RSA를 사용하고 있다. 하지만 RSA의 경우 보안을 위한 키의 길이 자체가 무선 환경에서는 적용하기가 현재로선 거의 불가능하다. 따라서 무선 PKI에서는 길이가 7~8배 짧으면서 동일한 성능을 나타내는 ECDSA가 주로 사용되고 있다.

국내에서는 이동통신 3사 모두 W-PKI 시스템을 이미 구축 완료한 상태이다. 하지만 아직 국내에서는 모바일 커머스가 활성화돼 있지 않은 상태이며, 앞서 말한 기술적인 한계 때문에 전폭적인 적용 자체에는 시일이 걸릴 듯 하다. 이에 대한 대안으로 W-PKI보다는 개인 단말기 번호 등을 이용한 키 생성을 통해 사용자를 인증하려는 움직임도 나타나고 있다.

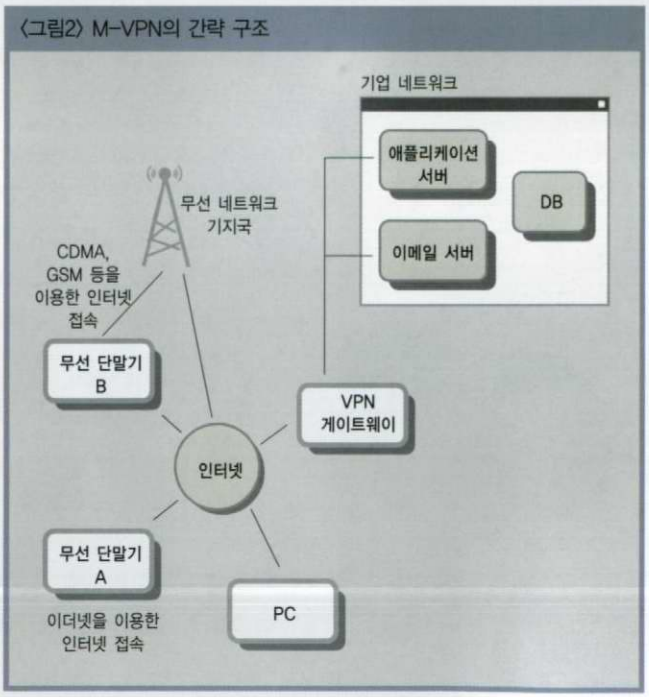
모바일 VPN, 무선랜에 대한 완벽한 암호화 기능 제공

M-VPN 역시 유선과 마찬가지로 VPN 국제 표준인 IPSec 프로토콜을 준수해야 한다. IPSec 프로토콜에는 세 가지 주요 보안 요소가 포함돼 있다.

AH(Authentication Header)의 경우 IP 데이터 그램에 대한 인증 정보를 제공하며, ESP(Encapsulation Security Payload)는 비밀성을 제공한다. 또 IKE(Internet Key Exchange)는 AH와 ESP에 채택된 암호화 알고리즘의 확장 가능한 교섭 기능을 제공한다.

VPN(IPSec)과 802.11(무선 전송 표준)의 결합은 최근의 무선 네트워킹 보안에 이상적인 솔루션이다. 이런 솔루션을 통해 무선 AP(Access Point)는 어떤 암호화 없이도 개방형 액세스로 구성될 수 있으며, VPN이 보안을 담당하게 된다.

〈그림2〉 M-VPN의 간략 구조



VPN 서버는 무선랜에 대한 캡슐화 기능과 인증 및 완벽한 암호화 기능을 제공한다. 그 결과 인증된 각 사용자는 네트워크 리소스에 대한 엔드 투 엔드, 완벽하게 보호된 투명성을 갖게 된다. VPN 서버는 중앙에서 관리할 수 있기 때문에 관리자의 업무 부하도 낮은 편이다. 또한 WEP이나 MAC 어드레스 필터링과는 달리, VPN 솔루션은 대량 사용자를 위한 확장이 쉽다. 게다가, 많은 기업들이 이미 자사의 기업 네트워크에 VPN을 구축했기 때문에 이를 무선랜으로 확장하는 것은 훨씬 경제적이다. VPN 접근 방법은 인터넷을 통한 DSL/케이블 모뎀 접속이나 공항과 호텔에서의 공중 무선 AP, 구내 무선 액세스 등과 같은 다양한 방법을 통해 기업 네트워크에 접속하는 사용자들을 처리하는데 있어서의 유연성을 제공해준다.

W-PKI와 M-VPN 이외의 보안 기술로는 단말기 보안 기술이 있다. 이 기술은 무선 단말기 사용자들을 위한 솔루션으로, 일반적으로 기기 분실과 데이터 손실의 경우를 대비하는 차원이다. 주요 수단으로는 암 · 복호화 또는 패스워드 등을 활용한다.

비용절감과 효율성 'M-VPN' 이점

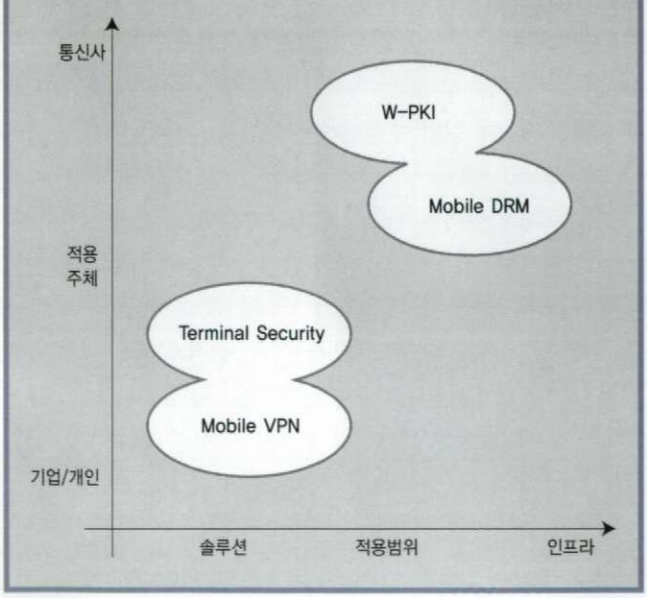
이상 살펴본 세 가지 무선 보안 기술들을 살펴보면 그 규모와 적용 대상 그리고 적용 범위에서 차이를 갖는 것을 알 수 있다.

W-PKI는 기본적으로 깔리는 인프라라 할 수 있다. 하지만 이 기술은 공인이라는 성격과 그로 인한 책임의 문제 등으로 인해 사실 사설 기업과 개인들은 구축을 생각하기 어려운 게 사실이다. 또한 M-VPN을 비롯한 다른 보안 시스템에도 W-PKI는 근간의 의미로 활용될 수 있다.

M-VPN의 경우는 대부분 기업에서의 활용이 유력시된다. 이미 많은 기업체들은 유선 VPN을 구축 활용 중에 있다. 따라서 비용 절감과 프로세스 효율성 제고를 위한 M-VPN으로의 확장은 그리 망설일 일은 아니다.

유선과 무선의 구분이 점차 모호해지고 있는 것은 주지의 사실이다. 보안 역시 그렇다. 무선 보안의 초창기에 그리고 지금까지도 상당 부분 유선의 그것을 수정하려는 것이 현실이다. 이러한 기조는 유 · 무선간의 문제뿐만 아니라 솔루션간 통합에 대한 문제도 제기하고 있다. 물론 이는 이동통신사 및 정부 등의 이해관계자들의 조율과 협조가 필수적인 요소들이다. 이 점은 무선 보안에 있어 흥미 있는 관전 포인트가 될 것이다.

〈그림3〉 무선 보안 솔루션 구분



모바일 비즈니스 확대에 '보안' 필수

그렇다면 이러한 상황에서 필자는 왜 모바일 DRM이란 것을 얘기하려고 하는가? 또 모바일 DRM이란 무엇인가? 왜 필요한가?

물론 앞으로 3회에 걸쳐 자세한 설명을 하겠으나 모바일 DRM의 출발은 전혀 기술적이지 않다는 것을 꼭 염두에 두길 바란다. 다시 말하자면 모바일 DRM은 콘텐츠 비즈니스의 확대, P2P의 파급력 증대 예상, 가치사슬 상의 이해관계자들의 헤게모니 싸움 등에 그 실질적인 시발점이 있다고 할 수 있다.

무선 보안 솔루션이 광범위한 네트워크 개념의 보안이라면 모바일 DRM은 철저하게 콘텐츠(파일 근간)에 결합돼 있다. W-PKI로 인터넷 뱅킹을 이용한다고 하자. 사용자나 인프라를 맡고 있는 이동통신사나 W-PKI가 돈을 만들어주지는 못한다. 단지 돈과 관련한 어떤 행위에 대한 안전성을 보장해줄 뿐이다. 사내에서 모바일 VPN으로 업무를 처리한다고 하자. 이 역시 보안 시스템이 어떤 부가가치를 창출하는 것은 아니다. 하지만 모바일 DRM은 다르다. 바로 돈과 연관돼 있다. 모바일 DRM 시스템은 돈을 만들어 주기도 하고, 돈이 새나가는 것을 막아주기도 한다.

앞으로 연재될 내용에 대해 독자 여러분들과 활발한 커뮤니케이션이 있길 기대하고, 모바일 DRM에 대한 여러분들의 이해가 증대될 수 있기를 기대한다.