한국컴퓨터정보학회지
제22권 제1호, 2014. 6.

임베디드 환경을 위한 SSL VPN

• 박재필(시큐위즈)

I. 서론

최근에 모바일 컴퓨팅 환경이 일상화되고 많은 사용자들이 모바일 디바이스를 이용하고 있다.

또한 폭발적으로 증가하는 모바일 이용자와 이에 대두되는 모바일 보안솔루션 시장에 벌써부터 많은 업체들이 뛰어 들고 있다. 또한 임베디드 장치를 사용하는 CCTV나 POS 단말기, 카드 단말기와 같은 경우에는 개인정보나 개인 사생활 정보가 담긴 데이터를 전송하게 되므로 보안의 필요성이 대두되고 있다. 그럼에도 불구하고 현재는 임베디드 장비를 보호하기 위한 보안 장비들은 전무한 실정이며 이에 따른 보안 위협도 점점 커져만 가고 있다.

이에, 기존의 가상사설망 Client 기술 한계를 극복하고, 모바일 환경 지원, 임베디드 모바일 클라이언트 기술을 적극 개발하여 모바일 단말의 보안성을 강화할 필요성이 대두되었다. 이에 대응하기 위하여 첫째, 모바일 디바이스에서 사용하는 여러 종류의 OS와 하드웨어에 호환되는 SSL-VPN 클라이언트의 개발이 필요 한다. 이를 위해서는 임베디드 및 모바일 OS에서 동작하는 가상 네트워크 드라이버의 개발이 필요하며 이를 제어하기 위한 제어 프로그램과 클라이언트 프로그램의 개발이 필요하다.

특히, 임베디드 시스템은 전 세계적으로 많은 수의 중요한 인프라들을 제어한다. 그 때문에 해커들이나 테러리스트들의 주요 공격 대상이 되곤 한다. 그러나 임베디드 시스템은 보안 이외의 동작에서 일상적으로 사용되는 임의적인 방어, 메커니즘, 절차들을 갖는다. 이는 일부 경우에는 윈도우즈나 리눅스와 같은 전형적인 기업 시스템보다 더 강력한 보안 메커니즘을 필요로 한다. 이에, 공중망을 이용한 임베디드 시스템에서 네트워크 보안을 위한 SSL VPN Client개발의 중요성이 대두되었다.

임베디드 시스템이란 간단히 말하면 특정한 기능을 수행하기 위한 하드웨어와 소프트웨어가 조합된 전자 제어 시스템을 이야기 한다. 예를 들면 카드 결제기나 ATM, IP 카메라, CCTV, 가전제품 등과 같이 특정한 기능을 수행하도록 만들어진 하드웨어에 이를 조작하기 위한 소프트웨어를 내장한 것을 임베디드 시스템이라 부른다. 초기의 임베디드 시스템은 그 구성이 매우 단순하였으나 최근에는 마이크로프로세서와 DSP(Digital Siginal Processing)칩이 사용됨에 따라 이를 제어하기 위한 임베디드 OS가 사용되게 되었다. 이런 임베디드 시스템 중에서도 네트워크 자원을 사용하는 시스템, 그중에서도 특히 중요한 개인정보나 사생활 보호가 필요한 정보를 담고 있는 카드 결제기나 ATM, IP 카메라, CCTV, 홈 네트워크 등의 시스템에서는 보안의 필요성이 시급히 필요한 실정이다.

II. 관련 연구

1. 관련연구

1.1 산업 및 시장의 특성

SSL-VPN은 간편하게 브라우저만으로 사용자가 기업자원에 리모트 액세스 하도록 구현된 솔루션으로, 차세대 기업 네

트워크의 보안 강화를 위한 최고의 보안기술이다. SSL VPN은 복합인증, 암호화 통신 및 모바일 클라이언트 지원 등 원격지 보안 통신에 필요한 제반 요건을 만족한다는 점에서 기존 VPN을 대체할 수 있는 유일한 대안으로 자리매김하고 있다.

VPN은 인터넷 네트워크 상에서 외부의 영향을 받지 않는 가상적인 터널을 형성해 완벽한 보안 환경을 제공하는 기술(터널링과 암호화)로 이를 대체할 신기술이 없는 한 VPN시장은 향후 10년간 지속될 것으로 전망된다. 특히, SSL-VPN은 기존 VPN의 보완제품에서 대체품으로 인식되기 시작했으며, u-IT인프라 구축 및 스마트폰 보안, M2M기기 활성화를 주축으로 2018년까지 성장할 것으로 전망된다.

표 1. 연도별 보안기술 현황

기술 구분	IPSec VPN	IPSec VPN VPN 서비스	IPSec+ SSL혼용	IPSec+ SSL혼용 SSL VPN	IPSec+SSL혼용 SSL VPN Embedded SSL VPN
년도	1997~ 2010	2000~	2004~	2007~	2014~

특히, 단일포인트 장비 중심에서 모바일 데스크(모바일 기반의 클라이언트) 중심의 업무방식으로 변화됨에 따라 VPN 기술은 무인 및 정보기기단말(Embedded System)에 VPN Client S/W를 탑재하여 보안성을 강화한 새로운 형태의 u-VPN 서비스가 활성화 되고 있다. 또한 네트워크의 진화에 따라 타 서비스와 융합되어 다양한 서비스의 허브 역할을 수행하게 될 것으로 전망되며, 주요사업은 다음과 같다.

- u시티, 지능형교통시스템(ITS) 구축(국가 간선도로망의 ITS화)
- ITS, 철도, 항공 등에서 활용 가능하도록 서비스망을 확장 구축
- 위치기반서비스(LBS)산업 및 첨단 교통물류산업(공간정보산업육성법, 제정추진)
- 건설업과 IT를 융합한 u시티 건설(IT와의 접목을 통해 고부가가치 신규시장 창출)
- 첨단정보통신망 등 u시티 기반시설 관련 시장을 형성
- 인텔리전트 빌딩과 관련된 도시민 대상 u서비스(u교통·u교육·u헬스)등을 집중육성
- 병원의 u-Healthcare 시스템 기반 구축 사업
- ATM 및 전기 사용량 원격 검침사업등의 초소형 M2M기기 보안 사업

1.2 국내·외 시장동향

- 기업의 모바일 도입 활성화

BYOD는 기업 시장에 많은 영향을 미쳤지만, 관리 및 보안 부문의 문제 때문에 일정 부분 제약을 받았다. 그러나, 기업이 검증한 제품 정보를 제시하고 선택하는 CYOD (Choose Your Own Device)가 확산되면서 점차 BYOD의 간극을 좁힐 것으로 보인다. 이를 통해 기업은 점차 기업용 앱 지원 및 서비스 등에 집중할 것이며, 실제 비즈니스 성장과 비용 절감 부분을 우선적으로 고려하는 기업용 모바일 환경을 추진할 전망이다.

2014년 국내 기업의 모바일 도입 시장(Enterprise Mobility)은 약 6.94조 원을 기록할 전망이다. 경기 침체로 기업들의 투자가 위축되고 있지만, 2017년까지 연 평균 4.7% 성장하여 2017년에는 약 7.67조 원의 시장을 이룰 것으로 예상된다.

- 사물인터넷(IoT) 시장 확산

미국 시스코(Cisco)가 2011년에 발표한 보고서에 따르면, 2008년에서 2009년 사이 전 세계 인구수를 인터넷에 연결되어 있는 단말기 수가 추월해 이미 IoT 시대에 접어들었으며, 향후 2020년에는 전세계 500억 개의 단말기가 인터넷으로 연결될 것으로 전망했다.

또한 스마트 혁명 이후 스마트 기기 확산, 통신모듈과 플랫폼 서비스 발전, 클라우드와 빅데이터와 같은 정보처리기술의 진화는 M2M/IoT시장에도 영향을 미치며 실질적인 성장기를 맞이 하고 있다.

글로벌 시장조사기관 가트너(Gartner)에서도 2013년 10월 IT기술의 시장성장 추이를 전망한 하이프 싸이클(Hype Cycle)에서 M2M이 관심고조기(Peak of Inflated Expectations)를 지나 현실적 재조정기(Trough of Disillusionment)에 접어 들며 2014년을 이끌 10대 전략기술 3위로 선정했다.

이러한 변화에 따라 국내 IoT 디바이스는 2020년까지 총

1억 600만대 정도로 증가할 것이며, 네트워크 연결 측면에서는 이 중 원거리 통신망인 WWAN이 17.5%, WiFi 및 블루투스 등 Short Range 가 69.2%를 차지할 것으로 전망된다.

2013년 시스코는 '사물간의 통신'으로 한정되었던 IoT 개념을 사물뿐만 아니라 사람, 업무, 데이터까지 모든 것들이 네트워크에 연결되는, '만물통신' Internet of Everything (IoE) 개념까지 확대했다. 이제 IoT는 공공재나 산업시설물에 한정되어 있던 수준에서 벗어나 자동차나 가전제품 등 일상생활까지 확대될 것이다. 스마트 가전, 스마트 카 등이 대표적인 사례다.

또한, 2013년부터 정부가 추진중인 창조경제 활성화의 일환으로 IT의 역할이 부각되면서 그간 정책적인 지원이 적었던 IoT 분야가 수혜를 볼 것으로 기대된다. 앞서 이야기한대로 비통신영역에서 정책을 추진하는데 있어 IoT기술이 활용된다거나, 스마트 그리드와 원격진료 활성화 등 정책지원이 활발하게 논의될 것이다.

□ 모바일 기기 확산에 따른 정보보안 및 개인정보보호

한국인터넷진흥원에 따르면 국내 정보보안 시장은 지난 3년 동안 지속적으로 58% 성장해, 2016년 2.6조원 규모에 이를 것으로 예상했다. 또한 모바일 보안 분야는 2013~2016년 사이 연평균 22%씩 성장할 것으로 전망했다. IDC에 따르면 전세계 정보보안 시장과 모바일 보안 시장은 같은 기간 각각 연평균 8%와 24% 성장을 전망했다.

그림 1. 정보보안과 모바일 보안 시장규모
(출처 : 한국인터넷진흥원)

모바일 기기의 대중화와 BYOD 등의 확산으로 정보보안 시장은 지속적으로 성장할 것이다. IDC는 2013년 전세계 스마트폰 및 태블릿PC 출하량이 12억 대에서 2017년 21억대 수준으로 증가할 것을 예상했다. 시스코는 지식근로자 1인당 BYOD 평균 대수는 2012년 1.3대에서 2014년 1.8대로 늘어날 것으로 전망했으며, VM웨어는 국내 직장인들은 1인당 평균 2.4대의 모바일 기기(노트북, 스마트폰, 테블릿)를 사용하는 것으로 나타났다(2013년 기준).

III. 본론

SSL VPN은 외부 네트워크에서 내부 네트워크에 있는 시스템 자원을 사용권한이 있는 일반사용자에게 안전하게 사용할 수 있도록 SSL 웹 표준 암호화 기술과 프록시 기술을 이용하여 개발된 SSL 기반 가상사설망(VPN) 기능을 제공하는 보안제품이다. 제품명은 SecuwaySSL VPN이며 크게 SecuwaySSL Server(이하 SSL-VPN server)와 SecuwaySSL Client(이하 SSL-VPN client) 두 부분으로 구성되어 있다. SSL-VPN Server는 Appliance 형태로 제공되며 외부 인터넷 망과 내부 네트워크가 연결된 지점에 설치되어 외부 네트워크에서 SSL-VPN Client가 내부 시스템으로 전송한 암호화 패킷에 대하여 복호화를 수행하고 내부 시스템에서 외부 네트워크에 있는 SSL-VPN Client로 나가는 응답패킷에 대한 암호화를 수행하여 가상사설망(VPN)기능을 제공한다. SSL-VPN Client는 일반사용자의 PC에 설치되어 운영되며 소프트웨어이며 SSL-VPN Server와의 암호화 통신을 수행한다.

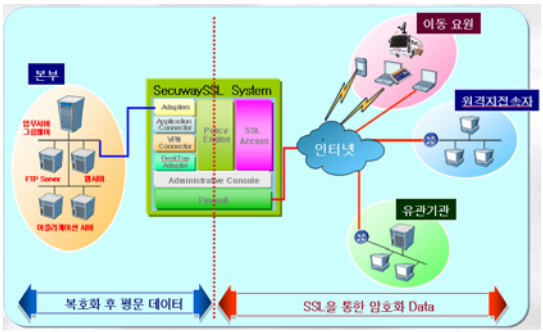

그림 2. 구성도

전체 구성도는 내부 네트워크와 외부 네트워크의 연결지점에서 운영되며, 외부 네트워크에서 내부 네트워크의 시스템 자원을 사용하는 사용자와 SSL-VPN 시스템 사이에 전송되는 데이터는 암호화되고, 내부 네트워크의 시스템 자원과 SSL-VPN사이에 전송되는 데이터는 평문으로 되어 있다. 시

스템은 관리자가 웹 브라우저를 통해서 시스템 설정, 사용자 등록 및 설정, 보안 정책, 보안 감사 기록 검토 등의 관리 업무를 수행할 수 있다.

위의 그림과 같이 SSL-VPN은 공중망을 이용하여 데이터를 전송하지만 암호화 기술을 사용하여 네트워크 트래픽을 암호화하여 허용된 사용자(또는 클라이언트)만 내부 자원에 접속할 수 있도록 기능한다. 해킹의 위협 및 무결성이 보장되어야 하는 서버들을 사설 네트워크 안쪽으로 숨겨 공중망에서의 직접적인 접속을 할 수 없도록 하고 클라이언트와 VPN 서버 사이에 암호화된 터널링을 생성하여 외부의 침입 및 데이터의 유출이 불가능 하도록 한다.

SSL-VPN 주요기능을 요약하면 다음과 같다.

표 2. SSL-VPN 주요기능

항목		내용
운영 모드	터널방식	Proxy 형태의 Web 방식, Gateway 형태의 Full 방식
특징	주요기능	SSL VPN + PKI + NAC
	암호화 가속방식	고성능 하드웨어 가속 방식
	프로토콜	SSL v2, SSL v3, TLS v1, WTLS
알고리즘	키 교환 방식	RSA (4096)
	암호화/복호화	SEED, ARIA
	Hash 알고리즘	SHA-2
ACL	기본적인 접근제어	ID/Password, 공인인증서(NPKI, GPKI), 사설인증서, OTP, USB Token, 핸드폰 인증, 선택/혼합
	추가적인 접근제어	그룹별/사용자 PC별/접속 IP별/요일별/시간대별 접근제어
	내부 서비스 제어	IP 대역/IP/PORT
	NAC	백신(선택) 설치여부/Windows 방화벽 사용 여부에 따른 접근제어
인증	공인 인증서	NPKI, GPKI 기본연동
	사설 인증서	CA/RA 기능 자체 내장(PKI 표준 준수)
관리	관리 화면	Web UI에서 일괄제어(Tcpdump, Tracert, Ping), 실시간 모니터링 Tool 제공(최대 6대)
	호환성	고객 DB(LDAP, Active Directory, Radius) 를 1:1 or N:1 연동, syslog 자동전송 기능
관리	가용성	사용자 로그인 페이지/인증서 매니저 이미지 변경 기능, 그룹별 Redirect 페이지 설정 기능
	운영의 편이성	프로세스 감시, 시스템 설정 정보 자동 백업 및 자동 외부 전송 기능, 사용자 일괄 등록, 그룹 일괄 변환, 무결성 체크 등
리포트	접근로그 시스템로그 감사로그	접근 사용자 정보, 로그인/로그아웃 여부, 내부 서비스 접근 정보, 관리자 감사로그 제공
	통계기능	사용자 접속 정보, 시스템 사용 정보, 사용자 단말정보, Traffic 정보의 통계 제공

제품은 4가지 모델(SecuwaySSL M50, SecuwaySSL M300, SecuwaySSL M1500, SecuwaySSL M10000)이 있다.

표 3. 제품사양

플랫폼 / 항목	Secuway SSL M50	Secuway SSL M300	Secuway SSL M1500	Secuway SSL M10000
CPU	Intel AtomTM D410 1.66GHz	Intel CoreTM 2 Duo 3.0GHz	Intel Xeon Quad-Core 2.53GHz	Intel Xeon Hexa-Core 2.4GHz X 2EA
Memory	DDR2 SDRAM 1GB	DDR3 SDRAM 4GB	DDR3 SDRAM 4GB	DDR3 SDRAM 16GB
운영체제	Fedora 15(Linux Kernel 2.6.38)			
HDD	SATA 500GB	SATA2 500GB	SATA2 500GB	SATA2 1TB
NIC	10/100/100 0B-TX, 4Ports	10/100/100 0B-TX, 4Ports	10/100/100 0B-TX 4Ports 1000B-SX 4Ports	10/100/100 0B-TX 8Ports 1000B-SX 8Ports

플랫폼 / 항목	Secuway SSL M50	Secuway SSL M300	Secuway SSL M1500	Secuway SSL M10000
제품 이미지				

IV. 결론

최근 들어 별도의 가입자 장비나 소프트웨어가 필요 없이 웹 상에서 간편하게 접속이 가능한 SSL기반 어플라이언스 구축 사례가 증가하고 있으며, 향후에는 SSL기반 중심의 보안시장이 자리 매김 할 것으로 추정하고 있다. 이처럼 SSL VPN의 활용이 늘어나고 있는 이유는 여러 가지가 있지만, 그중에서도 TCO의 절감과 생산성 향상에 도움이 된다는 것이 가장 중요한 요인으로 꼽히고 있다. 특히 SSL VPN은 웹 브라우저가 기본적으로 제공하는 보안 기술인 SSL기능을 이용해 VPN의 활용성을 한차원 높였다는 평가를 받고 있다. SSL-VPN은 웹 브라우저가 인터넷 접속이 가능한 위치의 사용자라면 누구에게나 VPN 접속이 가능케 하는 이동성을 제공해 생산성 향상과 개선된 효용성, 그리고 별도의 클라이언트 소프트웨어가 필요 없다는 편리함과 경제성을 앞세워 미래의 보안시장을 이끌어 나갈 기술로 인식되고 있다.

특히, 모바일 클라이언트 보안기술개발에 따른 유비쿼터스 업무환경을 구현하고, 국산 모바일 단말기 OS환경을 지원하는 보안장비 개발로 수입대체 효과가 기대되며 산업적 중요성은 다음과 같다.

첫째, 기업에서 스마트폰, 휴대폰, 모바일 패드, 노트북 등을 활용하는 모바일 인력수가 증가함에 따라 모바일 인프라의 확산으로 단말과 이동통신망 보호를 위한 모바일 VPN기술의 구현의 필요성이 더욱 대두되고 있다. 스마트폰의 활성화와 기업 내 모바일 사용자들의 증가로 무선 보안 이슈가 확대되고 있으며, 단말 전송 데이터 보호를 위한 모바일 VPN 확산될 것으로 전망된다.

둘째, 임베디드 시스템의 전송데이터의 보안을 위한 Embedded SSL VPN Client 개발이다. 특히, 정보기기, 물류, 금융 및 교통 등 아래와 같이 다양한 산업서비스와 융합된 u-IT인프라 고도화 사업으로 진화하고 있다.

- 무인자동화기기 및 금융단말시스템(ATM, POS,등)과 결합한 전자거래 보안솔루션
- 정보보안시스템과 SSL-VPN을 결합한 영상보안솔루션(영상전송 시 인증 절차를 거치고 암호화된 영상 데이터를 전송함으로써 영상정보 해킹이 불가능함)
- 지능형교통시스템(BIS, GIS등)과 결합한 데이터 암호화 솔루션
- u-Healthcare 시스템과 결합한 개인의료정보 보안솔루션(만성질환자의 의료측정 정보를 휴대폰을 통하여 의료기관에 전송하고 건강상태를 체크 및 피드백 시 데이터 암호화에 의한 개인정보보호)
- 모든 인터넷 망에 억세스하는 전자기기(냉장고, 자동차, 세탁기 ...)

현재 SecuwaySSL Client는 Windows XP, Windows Vista, Windows 2007, Windows 8, Windows 8.1 과 같이 MS 계열의 OS와 Linux OS에서 동작하도록 기술 개발이 되어 있어 그 활용분야가 데스크탑 PC로 제한되어 있다. 그러나 최근의 아이폰이나 구글 안드로이드 플랫폼, M2M초소형 기기 등과 같은 스마트폰의 보급이 급속히 늘고 있으며 과거의 일반 핸드폰 사용자들도 스마트폰으로 점점 옮겨가고 있는 추세이다. 또한 3G 서비스와 무선 인터넷의 보급으로 모바일 네트워크 인프라도 꾸준히 성숙되고 있는 상태에서 모바일 시장이 급속히 성장 할 것이라는 예측이 가능하다. 모바일 컴퓨팅 환경이 일상화되고 많은 사용자들이 모바일 디바이스를 이용하고 있으며 근 미래에는 이러한 추세가 폭발적으로 증가할 것이라고 예상되는 상황에서는 데스크탑 PC 뿐만 아니라 모바일 장비들도 아우르는 보안 기술 개발이 필수 불가결한 상황이다.

임베디드 디바이스를 사용하는 CCTV나 POS 단말기, 카드 단말기와 같은 경우에는 개인정보나 개인 사생활 정보가 담긴 데이터를 전송하게 되므로 보안의 필요성이 예전부터 대두되고 있다. 그럼에도 불구하고 현재는 임베디드 장비를 보호하기 위한 보안 장비들은 전무한 실정이며 이에 따른 보안 위협도 점점 커져만 가고 있다.

앞으로 예상되어지는 모바일 시장에 대응하기 위해서 현재 개발된 SSL VPN 클라이언트를 여러 기종의 모바일 디바이스 및 임베디드 장치에서 동작할 수 있도록 하는 것이 시급한 실정이다.

그림 3. IPSec VPN을 이용한 보안 네트워크

기존에는 임베디드 시스템에서 네트워크를 보안하기 위해서는 위 그림과 같이 IPSec VPN장비를 이용하여 보안 네트워크를 구축하였으나 이는 n대의 임베디드 시스템을 보호하기 위해서는 n대의 IPSec Client 장비를 구입하여야 하며 새로운 클라이언트를 설치 하기 위해서는 새로운 IPSec VPN 클라이언트 장비를 설치해야 하기 때문에 비용이 비싸고 확장성이 떨어진다. 또한 VPN-VPN 구간만의 암호화를 지원하도록 구현하기 때문에 보안성도 떨어지게 된다.

그림 4. SSL VPN을 이용한 보안 네트워크
(IP 카메라를 예를 든 것일 뿐
모든 임베디드 시스템에서 동일하다)

하지만 Embedded SSL VPN Client는 임베디드 시스템에 내장되어 작동함으로 인해 Client 장비 구매에 소요되는 비용을 절감하며 새로운 임베디드 시스템이 설치 된다 하더라도 내장된 롬에 프로그램이 포함되어 있으므로 손쉽게 설치하여 확장성이 뛰어나다. 또한 IPSec과 달리 Client-VPN 구간의 암호화를 지원하도록 구현된다. 또한 SSL-VPN Server 의 경우 기존 VPN은 싱글 코어만을 사용해 멀티 코어 제품에서도 온전히 그 성능을 모두 끌어낼 수 없었다. 멀티코어를 사용하여 각 코어의 독립적인 연산을 가능케 하여 Delay를 줄이고 최대 Thruput을 늘리도록 개발되어야 한다.

참고문헌

[1] 정보통신 산업 진흥원, 20013.2, Gartner, IDC, 2013

저자소개

박 재 필

1997: 단국대학교
전자계산학과 공학사.
2002: 홍익대학교
컴퓨터공학과 공학석사.
현 재: (주)시큐위즈 연구소장
관심분야: 네트워크 보안