모바일 VPN의 OTP를 이용한 모바일 화재 방재 모니터링 시스템 설계

LiQiGui*, 김영혁*, 임일권*, 강승구*, 이준우*, 김명진**, 이재광*
*한남대학교 컴퓨터공학과
**랜스(주)
e-mail:(qgli, yhkim, iklim, sgkang, jwlee, jklee)@netwk.hannam.ac.kr* ,
mjkim@lans.co.kr**

OTP in Moblie VPN using Mobile Fire Prevention Monitoring System Design

LiQiGui*, Young-Hyuk Kim*, Il-Kwon Lim*, Seung-Gu Kang*, Jun-Woo Lee*,
Myung-Jin Kim**, Jae-Kwang Lee*
*Dept. of Computer Engineering, Hannam University
**LANS Inc.

요 약

최근 스마트 모바일이 성장하면서 다양한 서비스들이 이루어지고 있다. 그 중에 모바일 오피스를 사용할 때 내부 망을 방문해야 한다. 그에 대한 보안 문제는 매우 중요하다. 본 논문은 모바일 기기가 내부 망에 방문할 때 사용자를 인증하기 위하여 통신의 보안 터널과 VPN(Virtual Private Network)기술을 사용하고, 모바일 기기가 내부 망에 방문할 때 OTP(One-Time Password)와 같은 동적인 패스워드 인증을 통해서 안전한 터널과 인증 서비스를 제공한다.

1. 서론

모바일 화재 방재 모니터링 시스템이란, 서버에 기록된 센서 데이터를 실시간으로 보여 주는 시스템으로, 모바일 기기로의 서비스를 위하여 개발되었다. 최근 모바일 시장이 크게 성장하고 있으며, 그 성장 속도는 MWC (Mobile World Congress)2010에서 확인할 수 있었듯이 일반적인 예상치를 넘어서고 있다(그림 1).

판매사	2009년 1사분기		2010년 1사분기		판매량 증가율 (%)
	판매량 (백만 대)	시장점유율(%)	판매량 (백만 대)	시장점유율 (%)	
노키아	16.9	40.3	24.0	38.1	42.0
RIM	8.0	19.1	11.2	17.8	40.0
애플	5.2	12.4	8.4	13.3	61.5
HTC	2.1	5.0	4.8	7.6	128.6
삼성	1.1	2.6	3.0	4.8	172.7
기타	8.6	20.2	11.6	18.4	34.9
합계	41.9	100	63.0	100	50.4

(그림 1) 2010년 2사분기 스마트폰 시장추세[1]

북미 모토로라, 중국 화웨이, 스웨덴 에릭슨 등은 2011년 휴대폰 시장의 30%가 스마트폰으로 구성될 것으로 추정하고 있다. 에릭슨의 경우 2015년 스마트폰 시장을 현재의 4배를 초과하는8~9억대 수준으로 전망하는 등 전 세계적으로 스마트폰 시장의 확산속도는 더욱 가속화될 것으로 예상된다(그림 2).

(단위 : 백만 대, %)

구분		2007년	2008년	2009년	2010년	2011년	2012년
휴대폰 판매대수		1,151	1,209	1,114	1,202	1,306	1,432
스마트폰	판매대수	121	143	178	254	351	469
	성장률	49%	16%	24%	43%	38%	34%
	비중	11%	12%	16%	**21%**	**27%**	**33%**

(그림 2) 세계 스마트폰 시장 전망(2007~2012)[2]

다양한 애플리케이션의 개발, 트위터 및 페이스북 등의 소셜 네트워크 서비스의 활성화, 무선인터넷 이용 증가 등으로 스마트 모바일이 활성화되고 있다. 스마트 모바일은 다양한 기능이 집약되어있어 이용자들이 보다 윤택하고 풍요로운 삶을 설계하도록 도와준다. 또한 애플리케이션을 기반으로 전화 통화는 물론 이메일 확인, 지도검색, 증강현실 등의 다양한 기능들을 제공한다. 즉, 과거 일반 PC에서만 처리할 수 있었던 일들을 이제는 언제, 어디서든 이용할 수 있게 되었다. 스마트폰을 사용 할 때 간단한 게임, 인터넷, Email 등의 용도로만 사용하는 것이 아니고 언제 어디서나 모바일 VPN 기술을 통하여 모바일 화재 방재 모니터링 시스템의 내부 망으로 접속하고 사용할 수 있어야 한다. 이 때 보안문제는 매우 중요한 사항이다. 안드로이드와 같은 개방형 플랫폼을 탑재한 단말의 등장은 제조사들에게 플랫폼의 단말 적용 편의성을 제공하지만 플랫폼 소스 공개에 따른 보안 취약점 노출위협이 증대될 수 있다. 또한, 앱스토어를 통한 애플리케이션 유통은 구매자와 개발자간에 애플리케이션 유통 편의성을 제공하지

만 악성코드가 포함된 애플리케이션을 보안성 검증 절차가 미비한 앱스토어에 올려 악의적인 바이러스 제작 및 유포 기회가 확대될 수 있다. 다양한 네트워크 접속환경 지원은 네트워크를 활용한 다양한 서비스를 제공할 수 있지만 스마트폰의 다양한 네트워크(Wi-Fi, Bluetooth, HSDPA)를 통한 감염 경로의 다양성을 제공할 수 있다. 본 논문의 목적은 화재 방재 모니터링 시스템 내부 망에 접속할 때 IPSec VPN을 통해서 안전한 통신 터널을 만들고 동적 OPT 암호로 신분을 인증 할 수 있다.

2. 관한 연구

2.1 가상사설망 VPN(Virtual Private Network)

가상사설망 VPN은 공용 네트워크를 통해 한 회사나 몇몇 단체가 내용을 바깥사람에게 드러내지 않고 통신할 목적으로 쓰이는 사설 통신망이다. 가상사설망에서 메시지는 인터넷과 같은 공공 망 위에 표준 프로토콜을 써서 전달되거나, 가상사설망 서비스 제공자와 고객이 서비스 수준 계약을 맺은 후 서비스 제공자의 사설망을 통해 전달된다. 가상사설망의 성장배경은 인터넷을 기반으로 한 기업 업무환경의 변화에 기인한다. 즉, 소규모 지역에서 문서만을 전달하던 업무처리 기반에서 하나의 건물 내의 네트워크를 이용한 업무로, 다시 본사와 다수의 지사 관계, 또한 지사는 국내 지사와 국외 지사로 확장되었다. 이들이 하나의 네트워크 구축을 위해 기존 전용선을 사용하는 방법에는 비용을 포함한 여러 가지 한계를 가지며, 전용선을 이용해서 네트워크가 구성되었다고 하더라도 네트워크 운영을 자체적으로 하는 것과 새로운 기술들을 도입하는 것 역시 기업의 입장에서는 상당한 부담이 될 수 있다. 또한 기존의 공용 네트워크는 보안과 관련해서는 서비스를 제공하지 않기 때문에 중요한 문서나 데이터를 전달하기에는 부족한 점이 있었다. 이러한 복합적인 이유가 가상사설망이 등장한 계기가 되었다. VPN과 IPSec(IP Security)은 VPN을 구현하기 위해 FrameRelay등의 여러 가지 방법이 이전에도 있었다. 그런데 그중에서 VPN의 주요기술로 IPSec을 소개하는 것은 TCP/IP기술이 현재 많은 네트워크의 표준기술로 사용되고 있고 차세대 인터넷 주소체계인 IPv6에도 헤더 부분에 기본으로 포함돼 있는 등 여러모로 가능성이 높기 때문 이다. IPSec은 TCP/IP통신의 약한 보안성을 강화하기위해 나온 보안방법으로 상호인증과 암호화서비스를 위해 강력한 암호화 기법들을 사용하고 있다. IPSec은 IETF에 의해 제안됐으며(RFCs 2401-2412), IP와 통합 되어있기 때문에 IP를 사용하는 어떤 응용 프로그램에서나 사용할 수 있다[3].

IPSec은 다음 세 가지 기능을 제공한다.

① 인증과 데이터 **무결성** : AH(Authentication Header) 프로토콜이나 ESP(Encapsulating Security Payload) 프로토콜에 의한 IP 데이터의 원본 인증과 무결성을 보장한다.

② 기밀성 : ESP는 암호화를 이용해 데이터의 기밀성과 제한된 트래픽 흐름의 기밀성을 제공한다.

③ 지역 간의 보안 통신 확립 : IKE(Internet Key Exchange, 일반적으로 ISAKMP/Oakley라고 불림)를 사용해 양단간의 보안 통신이 가능하고 필요한 암호화 키를 분배한다.

2.2 모바일과 VPN

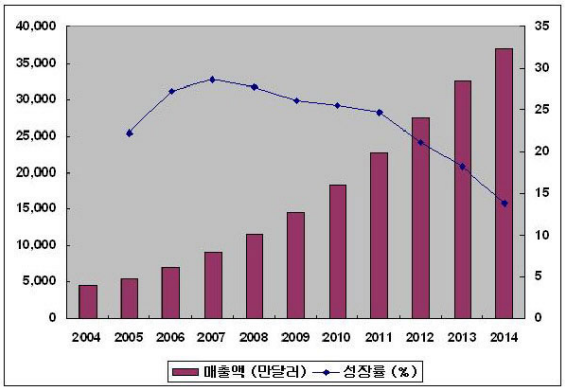
지금 주요한 스마트폰 즉 모바일 기기에도 이와 같은 역할을 하는 다양한 OS들이 각 단말 제조사들에 의해 채택되어 사용되고 있다. 대표적으로 palm, Linux, Nokia의 심비안, Microsoft의 Windows mobile, RIM의 Blackberry, 애플의 아이폰OS, 최근 시장을 확대하고 있는 구글의 안드로이드(Android) 등이 있다. 지금 대부분 스마트 모바일 OS는 모바일 VPN 지원한다(그림 3).

모바일OS	PPTP	L2TP	IPSec	OpenVPN
Symbian	PPTP	L2TP		
Android	PPTP	L2TP	IPSec	OpenVPN
iPhone,iPodtouch/iPad	PPTP	L2TP	IPSec	OpenVPN
Windows Mobile	PPTP	L2TP	IPSec	OpenVPN

(그림 3) 모바일의 VPN 지원현황

모바일 VPN 현상

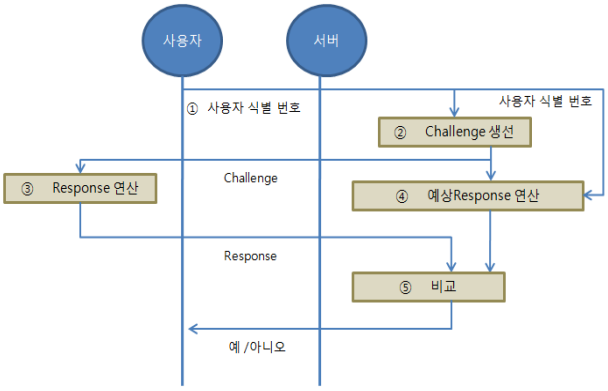
모바일 VPN 가상사설망이란 모바일 IP, IPSec 및 SSL 등과 같은 보안표준을 기반으로 무선 접속을 위해 배치된 특화된 VPN을 말한다. 시장조사 기관인 '프로스트 앤 설리'가 발표한 '전세계 모바일 VPN 제품시장' 보고서에 따르면, 전세계 모바일VPN 시장은 연 평균성장률 22.3%로 2007년 9000만 달러 매출에서 2014년 약 3억 7900만 달러에 달할 것으로 전망된다(그림 4), [4].



(그림 4) 모바일 VPN 전망

2.3 OTP 일회용 패스워드

일반적인 패스워드는 정적인 패스워드로 네트워크 도청으로 패스워드를 알아냈을 경우 불법적으로 재사용할 위험이 있다. 그러나 OTP는 필요에 따라 새로운 패스워드를 생성하기 때문에 네트워크 도청을 통하여 패스워드를 알아내더라도 더 이상 사용할 수 없으므로 이러한 위험을 방지 할 수 있다. 따라서 OTP는 정적인 패스워드 사용에 따른 위험을 해결하고 개인정보 유출에 따른 사용자 인증을 강화하기 위해 도입 되었다. OTP는 동적인 패스워드로 사용하기 위해서는 별도의 매체가 요구된다. 이 매체는 OTP를 생성할 수 있는 기능을 가지는 장치로 OTP토큰이라고 한다. OTP는 OTP생성매체에 의해 필요한 시점에 발생되고 매번 새로운 번호를 생성한다. OTP는 생성방식이 S/Key, 질의응답(Challenge-Response), 또는 시간동기화(Time-Synchronous)방식이 있다. 그 중 Challenge-Response방식은 사용자가 서버가 제시한 질의 값을 OTP토큰에 입력해 응답 값을 얻고 그 응답의 해당 값을 서버에 전송하여 사용자를 인증하는 방식이다[5]. 질의-응답 방식은 OTP토큰과 인증 서버 간에 동기화해 야 할 기존 정보가 없기 때문에, 동기화할 필요가 없으며, 사용자와 서버 간에 상호인증을 제공하는 방식으로 쉽게 확장이 가능하다(그림 5).



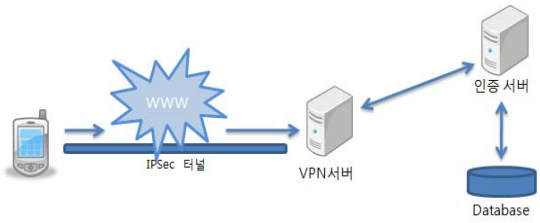
(그림 5) 질의 응답 인증 방식[6]

① 사용자가 인증 요구와 함께 사용자 식별 번호를 서버에 전달한다.
② 서버는 난수를 생성하여 Challenge로 사용자 에게 전달한다. 이와 동시에 서버는 사용자 식별번호에 해당하는 패스워드를 키 데이터베이스에서 꺼내 이것을 이용하여 난수를 생성한다.
③ Challenge를 받은 사용자는 그것을 자신의 패스워드로 암호화하여 서버에게 Response한다.
④ 서버는 예상 Response를 생성한다.
⑤ 사용자로부터 들어온 Response와 예상 Response와 비교하여 사용자를 인증한다.

3. 모바일의 VPN-OTP 인증의 구성

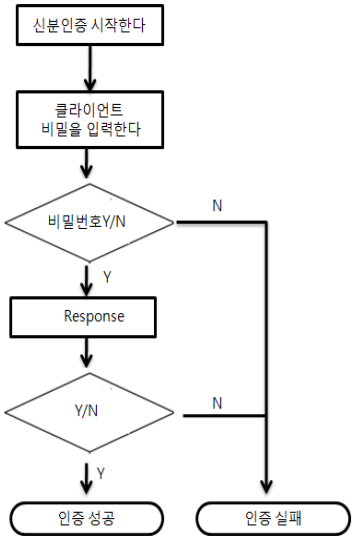
3.1 모바일의 VPN-OTP 인증의 구성

모바일의 OTP인증 구성도 부분(그림 6)은 인증클라이언트, VPN서버, 인증서버, 인증Database의 구성도이다.

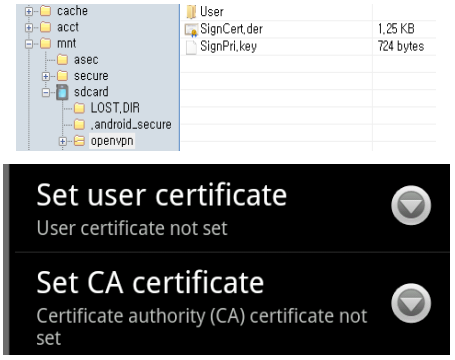


(그림 6) 모바일의 VPN-OTP 인증의 구성도

모바일의 인증 클라이언트는 OTP의 질의-응답 방식을 이용한다. 이 클라이언트는 OTP의 연산방법(그림 7), 기능 메뉴, 사용자의 신분ID, 인증서버의 필요하는 인증서(SDCARD/OPENVPN파일 안에 RSA공용키, 암호화 등 저장)를 포함한다(그림 8).

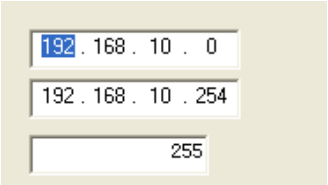


(그림 7) 클라이언트 인증 과정



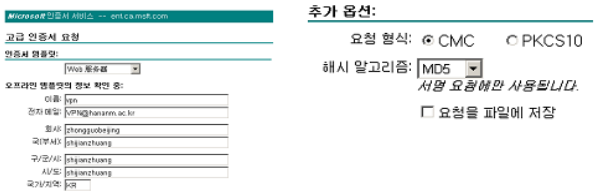
(그림 8) 인증서 저장와 읽는것 과정

VPN서버는 모바일에 내부IP주소 보낸다(그림 9). VPN이 구성될 때 IPSec 프로토콜을 통해서 안전한 터널을 제공한다. 또 VPN서버는 클라이언트에서 받은 인증 요청을 인증서버에 보낸다.



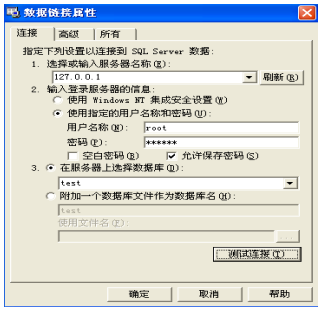
(그림 9) 내부 IP 주소 설치

인증서버는 모바일의 인증 클라이언트와 모바일의 신분 인증한다. 인증증서 발급하고 MD5를 통하여 암호화할 수 있다(그림 10).



(그림 10) 인증 증서 신청

인증 Database는 사용자의 등록정보 ID와 서버의 연산정보 등 저장한다(그림 11).



(그림 11) Database 연결

3.2 모바일의 VPN-OTP 인증의 구현 단계

① 먼저 사용자의 모바일에 VPN을 설치한다.

② 등록단계

모바일 화제 방재 모니터링 서버에 관리자와 사용자에게 모바일 인증클라이언트를 제공한다. 처음 사용하면 등록정보 개인정보 등 VPN터널로 통해서 인증서버 전송하고 인증 Database에 저장한다.

③ 인증단계

가. 사용자가 서버에 등록정보를 요청한다.

나. 서버의 인증 Database를 검사하고 로그인 정보가 맞으면 인증서버는 Challenge코드를 사용자에게 전달하고, 사용자의 정보 예상 Response코드를 생성한다.

다. 사용자가 Challenge코드를 받아 인증 클라이언트 비밀번호를 입력하고, 인증 클라이언트를 통해서 Response 코드 생성하여 인증서버에게 전달한다.

라. 인증서버는 사용자부터 받은 Response코드를 자기가 생성한 예상 Response코드와 비교한다. 맞으면 사용자에게 모바일 화제 방재 모니터링 시스템을 방문할 권한을 제공하고 그렇지 않으면 인증을 중단한다.

4.결론

최근 스마트 모바일이 성장하면서 화재 방재 모니터링 시스템에서도 모바일에 대한 수요가 증가하고 있다. 본 논문에서는 모바일 VPN서비스에 대해 확장된 서비스를 제공한다. 모바일을 통해서 화제 방재 모니터링 시스템에 접속할 때 IPSec VPN기술을 통해서 안전한 통신 터널을 제공한다. 또 모바일 인증 클라이언트를 통해서 사용자의 신분 인증할 수 있다. VPN와 인증기법은기존의Das 기법이 가지는 장점을 그대로 계승하여, ID 및 패스워드 테이블 도난공격에 대응할 수 있으며, 위장공격, 추측공격 등에도 대응 가능 한다.

본 연구는 중소기업청에서 지원하는 2009년도 산학연협력 기업부설연구소 지원사업(00037442-3)의 연구 수행으로 인한 결과물임을 밝힙니다.

참고문헌

[1] 나성욱, “스마트폰과 모바일 오피스의 보안 이슈 및 대응 전략” 한국정보화진흥원 p7

[2] 나성욱, “스마트폰과 모바일 오피스의 보안 이슈 및 대응 전략” 한국정보화진흥원 p7

[3] 최봉신, ″ FreeS/WAN을 사용한IPSec VPN 구현″ 인사이드 리눅스 2001/10/23.

[4] http://www.jeonpa.co.kr/news/articleView.html?idxno=2651

[5] 최동현 “일회용 패스워드(OTP)기술 분석 및 표준화 동향” 情報保護學會誌 第17卷 第三號 2007. 6

[6] 申東珪 “OTP방식을 이용하여 사용자 익명성 보장하는 소액결제시스템” p5