한국컴퓨터정보학회 하계학술대회 논문집 제23권 제2호 (2015. 7)

IoT기기를 위한 TLS VPN 구현

박재필O
O(주)시큐위즈 기술연구소
e-mail: foxyfeel@secuwiz.netO

An Implement TLS VPN for Internet of Things

J.P ParkO
OSECUWIZ CO. tech lab

● Abstract ●

본 논문에서는 최근 급성장하는 사물인터넷(Internet of Things, IoT) 시장의 안전한 원격 네트워크 통신을 위한 가상사설망(Virtual Private Network, VPN) 구축을 TLS(Transport Layer Security, TLS 1.0 또는 SSL 3.0) 프로토콜을 사용하여 암호화 기술, 터널링 기술을 적용한 인증 기반의 안전한 통신망을 제공하는 목적에서 기술개발의 고도화를 추구한다.

키워드: TLS VPN, IoT(Internet of Things)

I. Introduction

IoT용 TLS VPN 은 외부 네트워크에서 내부 네트워크에 있는 시스템 자원을 사용권한이 있는 일반사용자에게 안전하게 사용할 수 있도록 TLS 웹 표준 암호화 기술과 L3 터널링 기술을 이용하여 개발된 TLS 기반 IoT 전용 VPN 기능을 제공하는 기술이다.

이는 크게 서버와 클라이언트 두 부분으로 구성되어 있다. TLS VPN 서버는 어플라이언스 형태로 제공되며 외부 인터넷 망과 내부 네트워크의 연결 지점에 설치된다. TLS VPN 클라이언트가 외부 네트워크에서 내부 시스템으로 전송한 암호화 패킷을 복호화하고 그 반대의 상황에서의 응답패킷에 대한 암호화를 수행하여 VPN 기능을 제공한다. TLS VPN 클라이언트는 통신을 요하는 디바이스에 S/W 형태로 설치·운영되며 TLS VPN 서버와의 암호화 통신을 수행한다. 다음 그림은 본 제품의 구축 방안을 도식화한 구성 시나리오이다.

IoT 환경에 적합한 임베디드 IoT 클라이언트를 위한 기술 구현이 본격적으로 상용화됨에 따라 IoT 단말기 보안 강화의 필요성 역시 점차 중요 시 되고 있다. 기존의 VPN이 PC/Mobile용으로 국한되었다면 이제는 이러한 기술적 한계를 극복한 IoT 디바이스에 적합한 보안 대응책을 마련할 때인 것이다. 특히 IoT 단말기에서 사용하는 여러 종류의 OS 및 H/W에 호환할 수 있는 IoT 전용 TLS VPN 클라이언트 개발이 가장 시급하다.

위 그림과 같이 원격지에서 내부 네트워크의 시스템 자원을 사용하는 사용자와 TLS VPN 시스템 사이에 전송되는 데이터를 암호화하고,

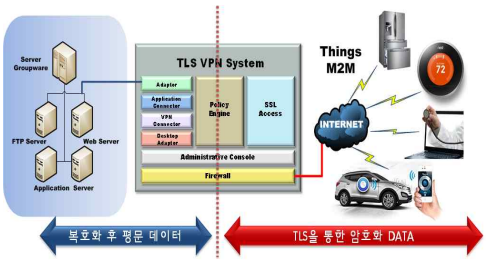

그림 320 IoT 환경을 위한 IoT用 TLS VPN 구성도

내부 네트워크의 시스템 자원과 TLS VPN 사이에 전송되는 데이터를 평문으로 구성한다. 시스템 관리자는 웹 브라우저를 통해 시스템 설정, 사용자 등록, 보안 정책/감시/검토 등의 관리 업무를 직접 수행할 수 있다. TLS VPN은 공중망을 이용하여 데이터를 전송하며 이때의 네트워크 트래픽을 암호화함으로써 허용된 사용자만이 내부 자원에 접속할 수 있도록 한다. 즉, 보안 위협에 취약한 공중망에서 직접 접속을 차단하고 클라이언트와 VPN 서버 사이에 암호화된 터널링을 생성하여 외부의 침입 및 데이터 유출이 원천적으로 불가능하도록 기능한다.

II. Preliminaries

1. Related works

1.1 국내 동향

포스트 스마트폰 시대가 개막함에 따라 아이폰이나 구글 안드로이드 플랫폼과 같은 모바일 기술 중심에서 M2M/IoT 환경을 위한 무선 라우터를 위한 보안 방안이 요구되고 있다.

특히, 무선 인터넷의 보급으로 M2M/IoT 네트워크 인프라도 꾸준히 성숙되고 있으며 급성장하는 M2M/IoT 시장 전망과 더불어 M2M/IoT 기기의 보안 기술 개발에 혈안을 올리고 있는 상황이다.

가상사설망 기술은 IoT장비의 임베디드 OS에 탑재하는 방식과 IPsec VPN 보안 장비를 추가하여 구축하는 방식의 경쟁 구도이다.

스마트 기기, 센서 등 다양한 단말 및 이기종 네트워크 활용하기 때문에 보안사고의 발생빈도는 더욱 커지고 있으며, 또한 네트워크 환경이 무선망으로 전환되는 등 사물 중심으로 폭 넓게 확산함에 따라 모든 기기의 센서와 네트워크의 정보 보안이 시급하다.

미래부에 따르면 우리나라 M2M/IoT 보안과 디바이스 기술 수준은 선진국과 비교해 2년 5개월로 격차가 심각하다[1].

III. The Proposed Scheme

M2M/IoT 서비스 사용 시 사람 또는 사물을 인증하는 단계에서 발생될 수 있는 프라이버시 침해 위협을 최소화하기 위해서는 전송 데이터의 암호화가 필수적으로 선행되어야 한다.

M2M/IoT 환경에서는 단순 통신 기능의 M2M기기에 암호화된 데이터 전송을 가능하게 하는 VPN을 탑재한 M2M 기기로 데이터의 안정성 확보가 필요하다.

공중망을 이용하는 통신상대와 가상사설망 통신을 수행할 때 전송되는 데이터를 보호하기 위하여 암호화, 터널링, 인증 등의 보안기능을 적용한다.

선행 연구에서 PC와 모바일 사용자에게 VPN 기술을 성공적으로 적용하였고, 이제는 M2M/IoT 시장으로 그 적용 범위를 확장하고자 한다.

IV. Conclusions

기대효과

기존 라우터에 적용하기 힘들었던 가상사설망 솔루션을 탑재해 보안 안정성 대폭 강화

무선 M2M 라우터를 사용하는 모든 사업에 본 기술을 적용하여 보안성 향상

유지보수 편의성 제고 및 다양한 공공 서비스에 대한 접근성 향상

산간 및 도서 지역처럼 유선 설치가 용이하지 않은 지역에 M2M 라우터를 활용하면 암호화된 데이터 기반의 다양한 공공서비스 이용

무선 M2M 라우터의 보안성 향상으로 인한 대국민 신뢰도 향상

최신 보안 기술, 무선 통신기술 등과의 기술 접목을 통한 통신 산업 부문의 첨단 기술 산업의 발전 유도로 국가 경쟁력 강화

다양한 OS플랫폼에 탑재가 가능하여 다양한 M2M/IoT 서비스로의 확장이 용이

기존 유선 VPN 대비 50%의 비용 절감

센서 단말 간 암호화된 데이터 전송을 위해 유선에서 무선 M2M 라우터로 대체

References

[1] 2015,3,15 대한민국 미래부