국산 개방형 구름 OS를 위한 TLS VPN Client

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

An Implement TLS VPN Client for Gooroom OS

J.P ParkO
OSECUWIZ CO. tech lab

● 요 약 ●

본 논문에서는 국내 OS시장의 편중화 현상을 해결하기 위해 개발된 개방형 OS 인 구름 플랫폼에서 동작 할 수 있는 가상사설망(Virtual Private Network, VPN) Client를 암호화 기술, 터널링 기술을 적용한 사용자 인증 기반의 안전한 통신망을 제공하는 목적에서 TLS[1](Transport Layer Security,TLS 1.2) 프로토콜을 사용하여 원천기술을 개발하며 이의 고도화를 추구한다.

키워드: 구름 OS, TLS VPN

I. Introduction

국내 윈도우 OS의 시장 점유율이 90%에 달하고 있어, 국가·공공기관 업무환경용 운영체제 개발의 필요성이 대두되어 국가보안기술연구소가 오픈소스 운영체제 기반 구름플랫폼을 개발 하였다. 이에 구름플랫폼을 위한 보안솔루션의 선행연구 필요성이 대두 되었으며 그중에서도 개방형 OS기반의 구름플랫폼에서 운용될 수 있는 SSL 기반 가상사설망 프로그램의 개발이 시급한 상황이다.

II. Preliminaries

1. Related works

1.1 국내 동향

현재 국내 가상사설망 기술은 대부분의 솔루션이 윈도우 계열 중심이다. 또한 배포 초기 단계인 구름 플랫폼은 윈도우 시장 대비 상대적으로 작은 시장 규모가 예상된다.

현재 국내 가상사설망 환경은 오픈소스 라눅스 기술 전반을 포괄하는 가상사설망 기술력이 미흡하고 구름플랫폼 환경에 적합한 가상사설망 원천기술이 부족한 실정이다.

구름 플랫폼은 개발 특성상 국가·공공기관 업무환경에 우선 적용될 가능성이 높으나 현재 이 환경에 적합한 가상사설망 원천기술도 부족한 상황이다.

이에 구름 플랫폼의 가상사설망 기술 대안으로 SSL-VPN 기술이 가장 적합하다고 판단되어지며 국내 도입여건의 특성상(인증 이나 국산 알고리즘의 사용등) 국내 원천기술 개발이 필요한 상황이다. 또한 이를 통해서 국가 공공기관 업무환경에 사용 예정인 구름플랫폼의 보안성을 강화해야 할 것이다.

III. The Proposed Scheme

가. 연구개발의 최종목표

1) 구름플랫폼용 가상사설망 클라이언트 S/W

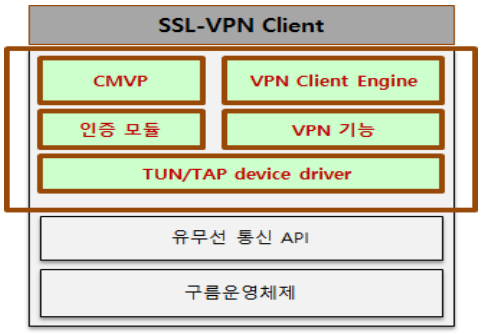

Fig 1. 개발하고자하는 프레임워크

2) 보안 요구사항 - 인증,기밀성과 무결성 보호,접근제어,종단 보안제어,침입탐지

3) 암호화 요구사항 - TLS 1.2프로토콜 지원,국산 암호 알고리즘(ARIA,SEED,LEA)지원,데이터 기밀성 유지 및 지원(ARIA-128-CBC 또는 LEA-128-CBC),데이터 채널 무결성 지원(SHA-256),인증(ID/PW 방식의 사용자 인증)

4) 가상사설망 서버 성능 - SSL-VPN 터널링 기능,국가용 장비 다급 이상(150Mbps)처리속도

5) 기대 목표 - 구름플랫폼 환경 구축으로 사용자 만족도 제고 및 활성화, 구름플랫폼 환경에 맞는 가상사설망 기술 확보로 국산 보안플랫폼 발전모델 마련

나. 구름플랫폼용 가상 사설망 개발

1) S/W 형태의 암호화 알고리즘 응용 개발

2) 암호화 알고리즘 및 가상사설망 모듈 연계

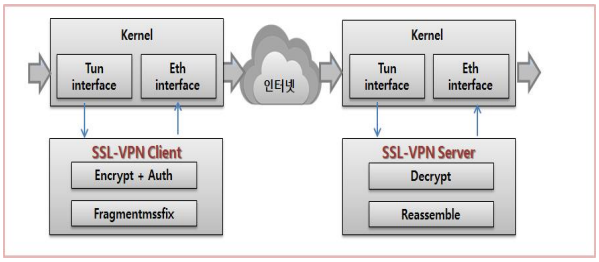

Fig. 2. 암호화 알고리즘 및 가상사설망(SSL-VPN) 모듈 연계도

3) S/W형태의 가상사설망 client 개발

- SSL-VPN 클라이언트는 통신을 요하는 클라이언트 단에 탑재될 수 있도록 개발
- SSL-VPN 서버와의 암·복호화 통신을 수행하도록 개발
- S/W형태의 가상사설망(SSL-VPN) 모듈은 API (Application Program Interface) 형태로 개발하여 클라이언트 OS에서 동작하도록 구현

4) 가상 네트워크 드라이버 개발

- VPN 클라이언트 모듈은 암호화 채널을 생성하기 위한 가상 네트워크 드라이버(TUN) 개발
- OS의 커널영역에 장착될 가상 네트워크 디바이스 개발
- User Space에 I/O 컨트롤러, 패킷 처리 엔진, 암/복호화 엔진, 압축엔진, 인증처리 엔진 개발
- 가상 네트워크 드라이버는 커널 영역에 장착될 모듈로써 네트워크 구성에 필요한 정보(Mac Address, IP Address)를 담고 VPN 서버와의 암호화 터널링 구성하도록 개발
- 인증 처리 엔진은 VPN 서버에 접속될 사용자의 객체를 확인하는 수단으로써 ID/PW 기반의 접속을 할 수 있도록 하고 클라이언트 장비의 유효성을 확인하기 위해 '클라이언트의 인증 값'을 작성하도록 개발
- DHCP를 통해서 VPN에서 사용하는 가상 IP를 할당받고 VPN 서버와 암•복호화된 데이터를 처리할 수 있도록 개발
- C언어를 사용하여 개발된 리눅스용 클라이언트를 구름 OS에서 동작하도록 포팅
- VPN 서버에서 인증을 거친 후 가상 네트워크 드라이버에 가상 IP를 할당하고 암호화 알고리즘을 사용하여 터널링이 맺어지도록 개발

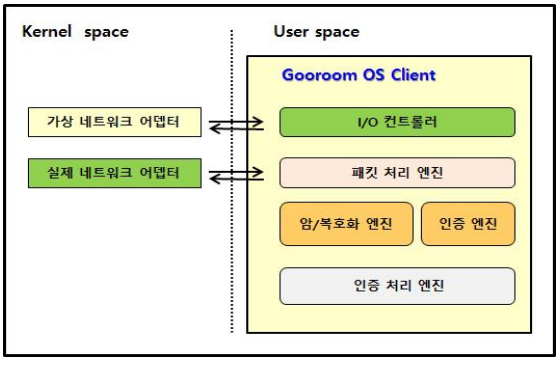

Fig. 3. 가상네트워크 드라이버 구조

5) 사용자용 GUI 개발

- SSL 기반 VPN 구름플랫폼 접속 프로그램 개발
- 기존 Command line 방식이 아닌 Gooroom OS 1.0 환경에서 이용할 수 있도록 GUI 개발
- 사용자 프로그램 자동설치 및 자동 업그레이드 가능하도록 개발
- 로그인 전 VPN 망 연결 기능
- GUI 접속 프로세스
  - 사용자 화면에서 '구름OS 클라이언트' 아이콘 더블 클릭 실행
  - URL란에 접속하고자 하는 서버의 IP를 입력 후 로그인 버튼을 클릭하여 다음페이지 이동
  - 아이디와 비밀번호를 입력 후 로그인 버튼 클릭하여 해당 서버에 접속
  - 로그인 후에 즐겨찾기 페이지에 표시됨
  - 즐겨찾기 목록에서 접속하고자 하는 페이지를 더블 클릭하여 바로접속
  - 정상 및 비정상 접속 확인 아이콘 생성(정상: 초록색, 비접속: 노란색)

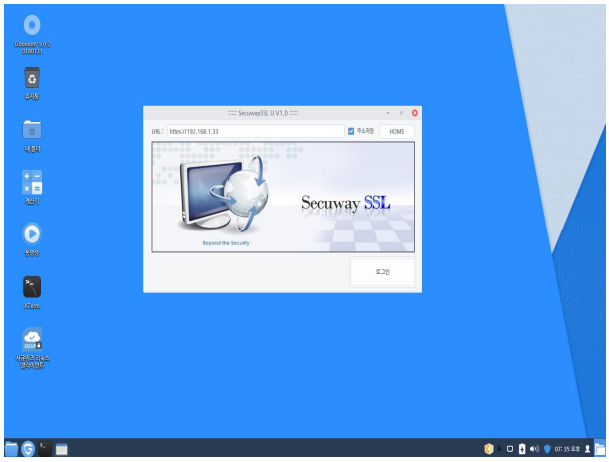

Fig. 4. 구름OS 클라이언트 GUI 실행 화면

IV. Conclusions

본 연구의 목표는 오픈소스 기반의 국가·공공을 위한 구름플랫폼용 가상사설망 개발에 있다. 이를통해 초기 배포 단계인 구름플랫폼 인프라의 보안성을 향상 시키고 국가 공공기관 구름플랫폼 사업 활성화의 기반을 조성하는데 기여할 수 있을 것이다.

연구 결과물(SW)은 구름플랫폼 패키지 저장소를 통해 오픈소스로 공개하여 구름플랫폼 보안솔루션 개발에 기여할 수 있을 것이며 나아가 구름플랫폼 가상사설망 시장 확대에 따른 국가 경쟁력 확보에 기여하리라 기대되어진다.

REFERENCES

[1] T. Dierks, "The Transport Layer Security (TLS) Protoco l

Version 1.2" IETF, RFC52461, August. 2008.