김일성종합대학학보
(자연과학)
주체103(2014)년 제60권 제9호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 60 No. 9 JUCHE103(2014).

Android에서 핵심부비의존암호화를 위한 IPSec VPN의 한가지 구성방식

김문일, 최혁철

가상전용망(VPN)은 신뢰할수 없는 공용망으로 련결된 두 말단사이에 신뢰할수 있는 통신통로를 구축하기 위한 전용망이다. 그중의 하나인 IPSec VPN은 IP보안규약(IPSec Protocol)을 리용하여 말단사이의 안전한 보안통로를 구축해준다.[1, 2]

Windows, Linux와 같은 범용조작체계에서 표준으로 제공하는 IPSec VPN에서는 조작체계가 지원하는 여러가지 암호화알고리듬을 리용하여 인증, 자료암호화를 진행하게 된다.

론문에서는 Android조작체계에서 핵심부의 표준암호화알고리듬에 의존하지 않고 우리식의 암호화알고리듬을 리용한 IPSec VPN을 실현하기 위한 Android용 IPsec VPN의 구성방안을 제안한다.

1. Linux에서의 IPSec VPN의 구성

Android는 Linux기반 공개원천조작체계로서 판형콤퓨터, 지능형손전화기를 비롯한 많은 이동정보장치들의 조작체계로 리용되고있다. 먼저 Linux핵심부에서 IPSec VPN실현방식에 대하여 고찰하자.(그림 1)

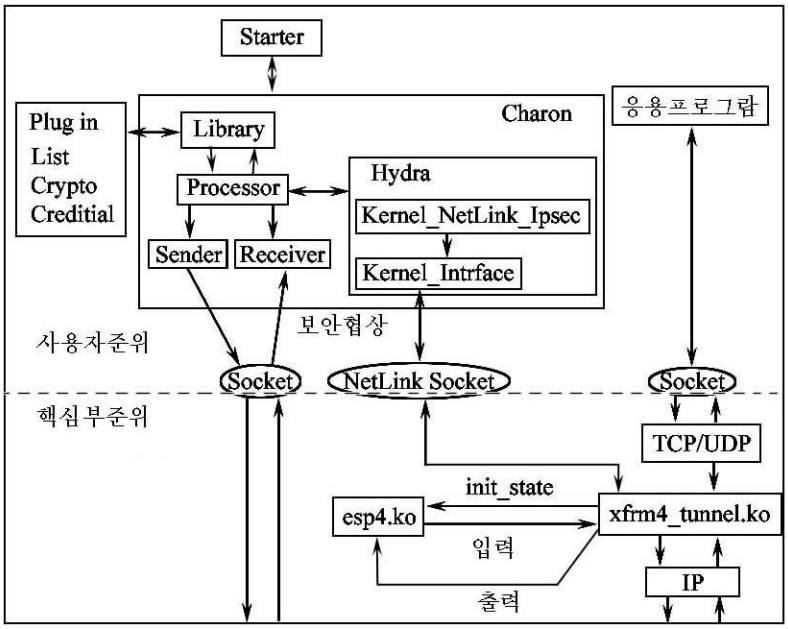

그림 1. Linux조작체계에서의 Ipsec VPN동작방식

그림 1에서 보여준것처럼 Linux조작체계에서는 핵심부준위에서 제공하는 파케트려과기능을 리용하여 전송층과 IP층사이의 파케트를 포획하여 핵심부준위에서 필요한 자료변환을 진행하고 IP층을 거쳐 파케트를 전송한다. 또한 자료의 포획과 변환이 핵심부준위의 구동프로그람들에 의하여 진행되며 사용자준위의 응용프로쎄스는 보안협상과정에 확정된 보안열쇠와 암호화알고리듬들을 특정소케트(Netlink Socket)를 통하여 핵심부준위에 전달하는 기능만 수행한다. 그러므로 자료부암호화에 리용되는 암호화알고리듬을 갱신하려면 핵심부의 표준암호화서고를 재구축하여 리용할 필요가 제기된다.[1]

다른 한편 Linux와 같은 일반콤퓨터용공개원천조작체계에서는 사용자가 필요에 따라 핵심부모듈을 재구축하여 삽입, 리용하는것이 큰 문제로 제기되지 않는다.

그러나 Android와 같은 휴대장치용 조작체계에서는 핵심부모듈을 갱신하는것이 일반사용자들에게 허용되지 않으며 따라서 Android조작체계에서 우리 식의 암호화알고리듬을 리용한 Ipsec VPN을 구축하려면 핵심부의 암호화알고리듬에 의존하지 않고 사용자준위에서 IP자료부암호화를 실현하기 위한 방안이 필요하다.

2. Android에서 IPSec VPN의 구성

Android에서 보안협상단계의 통신은 Linux에서와 동일하게 일반UDP소케트를 리용하여 진행되는데 Android에서 ESP파케트암호화에 표준Linux핵심부가 제공하는 암호화알고리듬이 아닌 우리 식의 암호화알고리듬을 리용하기 위하여 우리는 Linux핵심부가 제공하는 Tunnel기구(가상적인 Tunnel장치와 그것을 조종하기 위한 구동프로그람)와 미정소케트(raw socket)를 리용하여 IP파케트의 자료부(payload)를 Android의 Native준위에서 암호화하기 위한 구성을 제안한다. IP파케트의 payload를 사용자준위에서 암호화하기 위한 구성방법은 그림 2와 같다.

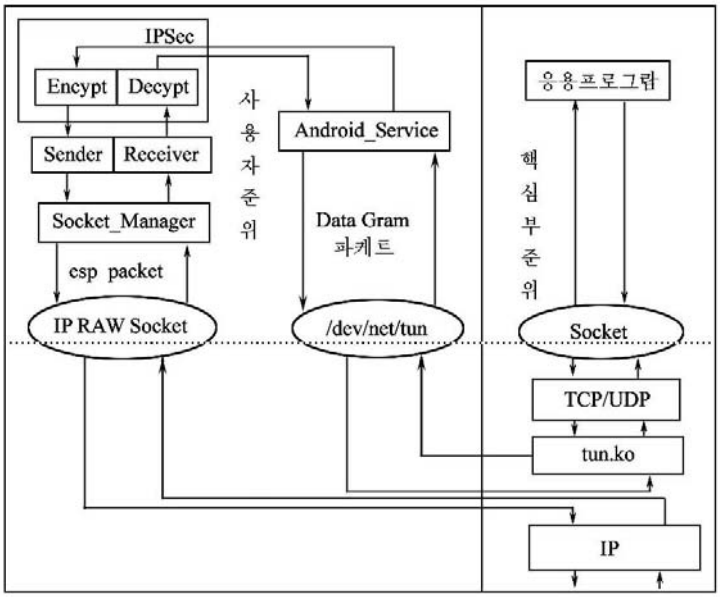

그림 2. Android에서 IP자료부의 암호화/복호화를 위한 구성

그림 2에서 응용프로그람으로부터 일반소케트를 통하여 전송층까지 전달된 자료부(payload)는 Tunnel장치에 의하여 tun장치화일에 쓰기된다. 이때 tun장치화일에 대하여 읽기대기중이던 android_service모듈은 이 자료를 읽어들여 native준위의 IPSec모듈에 전달하며 IPSec모듈에서 사용자가 정의한 암호화알고리듬을 통하여 암호화된 자료는 socket manager를 통하여 미정소케트를 통하여 IP층에 전달된다.

한편 수신파케트에 대해서는 반대로 미정소케트를 통하여 직접 Native층으로 전달된 암호화된 자료부(payload)를 복호화하여 tun장치화일에 저장한다.

tun장치화일을 통하여 전달된 복호화된 자료부는 Tunnel기구를 통하여 전송층으로 올라가게 된다.

전체적인 Android용 IPSec VPN프로그람의 구성도는 그림 3과 같다.

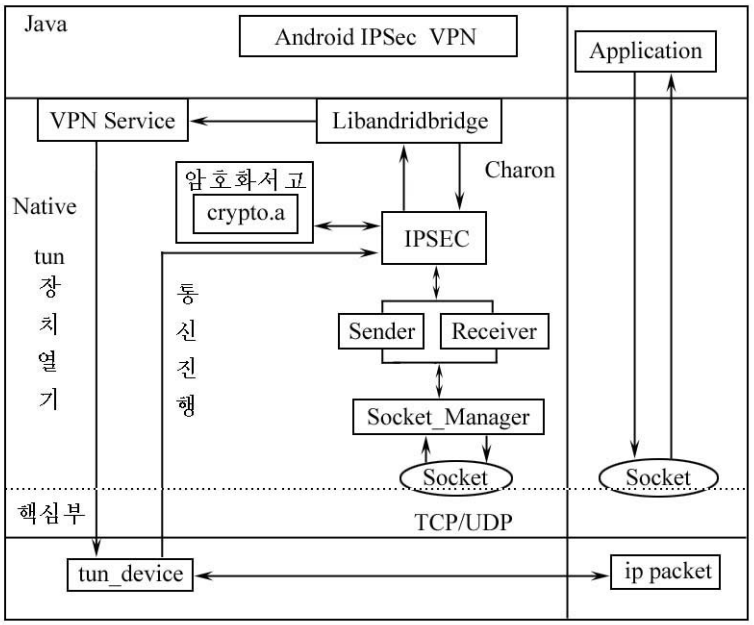

그림 3. Android IPsec VPN구성

그림 3에서 보는바와 같이 Tunnel장치를 리용하면 핵심부준위의 IP파케트가 사용자준위의 IPSec프로쎄스에로 전달되며 전달된 파케트에 대하여 사용자준위에서 전용암호화를 진행할수 있게 된다.

맺 는 말

Tunnel장치가 제공하는 IP파케트포획기능을 리용하여 Android용IPsec VPN의 자료부암호화알고리듬을 표준암호화가 아닌 우리 식의 전용암호화알고리듬을 리용할수 있는 구성방안을 제기하였다.

참 고 문 헌

[1] www.strongswan.org/docs/linuxTag2013-strongSwan.pdf, 2013.

[2] Jianwu Wu; ETP International Conference on Future Computer and Communication, 2, 2009.

주체103(2014)년 5월 5일 원고접수

An Architecture of Android IPSec VPN for Kernel-Independent Encryption

Kim Mun Il, Choe Hyok Chol

Using IP packet capturing function supported by Tunnel device of Android, we proposed an architecture of IPSec VPN client, which can use our custom algorithm for IP payload encryption instead of standard algorithms.

Key words: IPSec VPN, Android