The Mobile Terminal Security Access System Based on IPSec VPN

Di Zhao[1,a], Xin He[2,b] and Yunjun Li[1,c*]

[1]Department of Computer Science, Yanbian University, Yanji, 133002, China

[2]Shanghai Information Security Engineering Technology Research Center, Shanghai, 201204, China

[a]843469524@qq.com

[b]459248901@qq.com

[c*]Corresponding author: yjlee@ybu.edu.cn

Keywords: IPSec VPN; mobile terminal; replacement algorithm of cryptographic

Abstract. Based on IPSec VPN technology, we propose a scheme for realization of mobile terminal security access system. The scheme, which combines with SM2, SM3 and the IPSec, realizes the establishment of the IPSec VPN client data communication, and the client-server security communication functions by using the replacement of cryptographic algorithm and VPN interface technology. The security access system consists of two parts: mobile terminals and the application server.

In this paper, we analyze IPSec, IKE negotiation process, and the replacement of cryptographic algorithm on both client and server side, and then propose a new scheme of security access system. The experiments demonstrate the new system provides safe, reliable, and accurate data communication.

Introduction

With the development of mobile Internet technology and the mature of communication infrastructure, mobile terminals have become the handheld terminal tools that combine of calls, status representative, information acquisition, electronic payment, and other functions. At the same time, they are also facing some security challenges, such as funds stealing, privacy stealing, virus spreading and so on. At present, the transmission of wireless communication networks which based on commonality of limited security mechanism cannot guarantee the information security. Therefore, it is necessary to study and improve secure access system for mobile terminals, to protect user data.

In this paper, based on IPSec protocols and cryptographic algorithms, we employ *C/S mode* and *IPSec VPN* technology. The clients are mobile terminals with Android system and SDKEY, and PC with Linux system as the server. The system by calling underlying VPN interface of Android to realize authentication and security transfer functions between client and server. The system can be applied to government agencies and large enterprises for secure handling of related sensitive business.

Design of the Overall System

The system employs C/S model which mainly divides into client and server, as shown in figure 1. Users can connect IPSec VPN with Wi-Fi through configured client. The mobile terminals establish secure channel between customers and IPSec VPN server, transmit encryption data, so as to connect internal server security. Application server port includes two parts, the access server and application server. The access server receives connection request from mobile terminals, after finishing the identity authentication of users, builds a safety transport channel between mobile terminal and the access server. After decrypting the encrypted data send from the terminals, it forwards them to the application server, for ensuring the connection and transmission of data resource security.

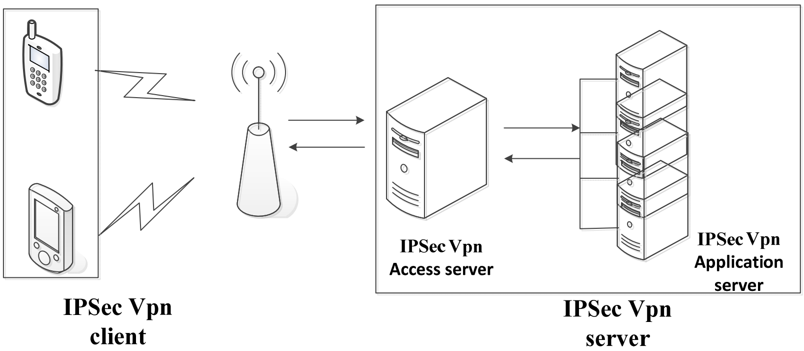


Fig.1 System Structure

Basic Idea of Replacing Code Algorithm

The IPSec (Internet Protocol Security) invocation structure is divided into user layer and kernel layer in Linux environment, as shown in figure 2. Firstly, when the upper user space received the IPSec request, it would negotiate with IKE and made the kernel layer to set up SA in negotiation process. Secondly, SPDB (security policy database) and SADB (security alliance database) set the choice of AH/ESP protocol, negotiation mode and processing method of IP packet, etc. Finally, Linux kernel network system feedback the information to IKE module, after completing an IKE negotiation, for dealing with network application according to the results of the negotiation. In order to realize the entire security access system, the domestic encryption algorithm would be used to replace the original international IPSec encryption algorithm. Through the study of IPSec protocol invocation, the calling process of cryptographic algorithm is mainly divided into two parts: the kernel space, after IPSec connection process used data encryption module to encrypt user data; the user space, it phase called encryption algorithm to set up a SA in IKE negotiation process. Therefore, the code algorithm was to be replaced by the key in IKE negotiation process of IPSec, that is to say, the main idea is replacing the original algorithm during negotiation stage.

Supposing that the first stage of IKE negotiation uses the main mode, the second stage uses the fast mode, so that in the entire IKE process it needs to send 9 packages. Message encapsulation format as shown in figure 3, the payload is the load content of IKE negotiation. In the first stage of the negotiation, it needs to send 6 packages to establish sharing policy and SA of key that can protect both sides of consultation. Corresponding packaging format, the content of the first package as follows: isakmp header; sa payload; proposal payload; transform payload. The package defines these things such as the encryption algorithm, the method of authentication, the authentication and integrity algorithm, survival time of SA, NAT, the cookie value and related strategies. The content of the second package is similar to the first package, includes the cookie value of response port. The third package and the fourth packet exchange the DH algorithm negotiations public/private key on sides. Generated secret key based on public key, private key and some parameters, they encrypt the symmetrical keys and authenticated keys. Three keys are generated in the process, SKEYID_D, SKEYID_A and SKEYID_E. The fifth and sixth packages are used to verify the equivalent identity which includes the source ID of certification and authentication keys. After the first stage IKE SA certification consultation authentication succeeded, the seventh and eighth packages would send new keys and negotiate a set of IPSec SA strategy that would be used to encrypt database of users. The ninth package employed SKEYID_E for encrypting. Its mainly content is the data confirmation message of the eighth package, used to verify the liveness of responder. Figure 4 shows the first phase and second phase process of IKE negotiation.

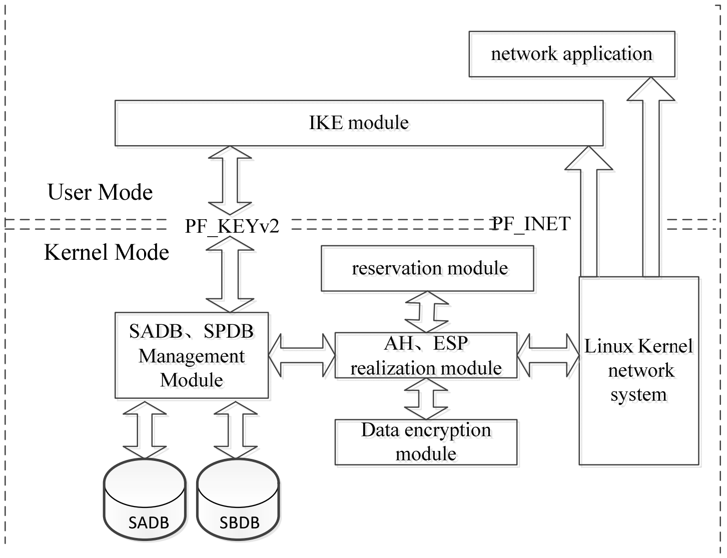


Fig.2 Linux IPSec Invocation Structure

Preamble	Etherent	S network IP	O network IP	UDP-500	Palyload	footer

Fig.3 IKE Packet Encapsulation

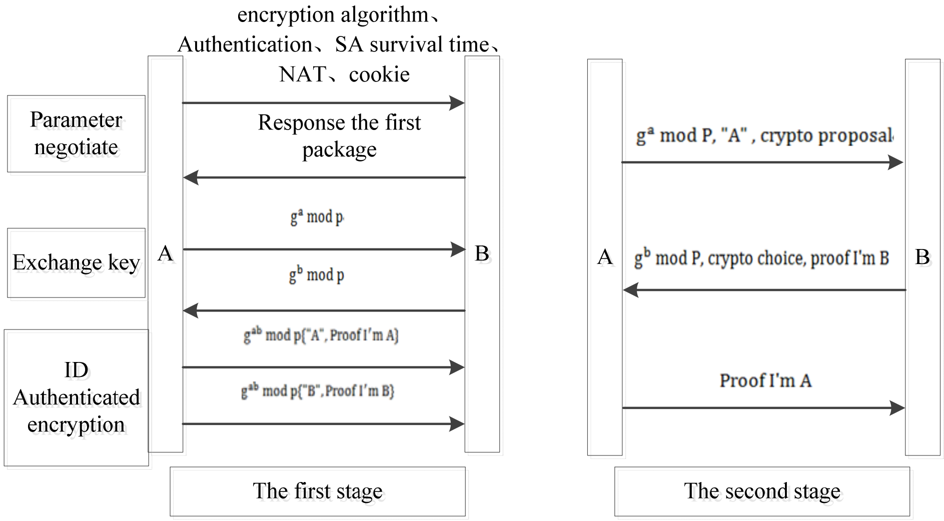

encryption algorithm、Authentication、SA survival time、NAT、cookie
Parameter negotiate
Response the first package
Exchange key
A
B
g^a mod p
g^b mod p
ID Authenticated encryption
g^{ab} mod p{"A", Proof I'm A}
g^{ab} mod p{"B", Proof I'm B}
The first stage
A
B
g^a mod P, "A" , crypto proposal
g^b mod P, crypto choice, proof I'm B
Proof I'm A
The second stage

Fig.4 IKE Negotiation Process

Design of Encrypted Access System on Mobile Terminals

Design of the Client IPSec VPN Software. This system based on the client with root permission of Android 4.x, for the first time using the client needs to configure the L2tp/IPSec PSK, users need install on the client certificate, add users and SD card encryption by network initialization, and then send connection requests to the server. After consulting with the client, the server to establish VPN channel, the client began to real-time monitor the user operation. If the user operation, the client IPSec VPN software authenticates whether the user has a corresponding operation permission by password and certificate validation, after authenticating access the password interface and to execute the specified operation. If there is no user action, the client keeps listening in the background.

After analyzing the call trace of MD5 algorithm, gets MD5 interface function mainly reserved in <SRC/raccoon/crypto_openssl.c>file, two sets of interface were found by the research, as shown in table 1.

Table.1 MD5 Algorithm Interface

Traditional Interfaces	EVP Interfaces
eay_md5_init()	init(EVP_MD_CTX *ctx)
eay_md5_update(c, data)	update(EVP_MD_CTX *ctx , const void *data , size_t count)
eay_md5_final(c)	final(EVP_MD_CTX *ctx , unsigned *md)
eay_md5_one(data)	EVP_md5(void)
eay_md5_hashlen()	

When calling MD5, the client will use the traditional interface, but calling the HMAC_MD5 will use the EVP interface. In order to call the EVP interface that need to replace two sets of interface synchronization in eay_md5_one () function of traditional interface. EVP interface defined in <m_md5.h>. In addition, as a result of MD5's length by calculating is different from SM3, so, except for modifying the return values of eay_md5_hashlen () function, also need to modify HMAC_MD5 function interface, because of client calling MD5 algorithm calculation message authentication code.

One of the key techniques on client software is the password service interface that to call SDKEY encryption algorithm in the Android application layer and provide the upper application with symmetric encryption, asymmetric encryption, digital signature and certificate. The encryption interface of encryption card cannot be used as application development API directly, therefore, using the NDK technology to add the encryption algorithm by the hard way.

Due to the difference of permissions which provided by Android manufacturers, for getting system permission to do the sensitive operations on Android, it needs to sign System, but the signature system can't be get by ordinary users. So this aim at researching the generality of Android 4.x version, the main idea is access NDK to get permissions with the process of packaging function interface using the Shell in the Linux command line, to solve the problem of the underlying permissions. In order to start RACOON and MTPD service, for example, to use Linux terminal "setprop ctl. start raccoon" modify permissions on the kernel, and then to "property_set ("CTL. Start", "raccoon")" in C layer to encapsulate startup command. Finally the Android applications layer uses the command "SystemProperties. set (" ctl start. racoon ")"to start the IPSec.

Design of the IPSec VPN application on server. Server development using Ubuntu10.04 32 as the operating system, the software bases on OpenSwan that combines with X12tpd. The first time for using, server software also needs to do the system configuration, after configuration, the establishment of a real time monitor the VPN request. If requested, validate the password and security certificate matches, both these pass verification and after completing of IKE negotiation, VPN set up successfully. The next step is to encrypt data that on the client, forward to the application server, to ensure the security of the user data.

The IKE negotiation on sever process is different from client with IPSec-tools, OpenSwan IKE process calls the kernel code library in the Pluto directly. Crypto used algorithms library in the first stage, and the Kernel and Kernel_Netlink is used in the second stage that to negotiate with the Kernel communication algorithms library. As for Cryptographic algorithms' replacement on server, replace with SM3 algorithm respectively two stages algorithms library called function interface.

The first stage, replaces old mark with SM3, the location of the mark as shown in table 2. Accordingly, add predefined "transform" on the corresponding position "db_attr" items. In accordance with the above method, the modified RSA certificate authentication corresponding "oakley_trans_rsasig_attr", pre shared key corresponding "oakley_trans_psk_attr", RSA certificate or pre Shared key corresponding "oakley_trans_pskrsasig_attr ".On the other hand, registering SM3 algorithm in Crypto, modify "encrypt_desc" structure, replace the original algorithm. Among them, the main realization of interface function is do_sm3. Finally, initialization "init_crypto", "ike_alg_add" part use to register the structure and the SM3 algorithm in Crypto.

During the second stage, first registered in SPDB, and then add algorithm to "espa_trans" array. To OpenSwan identify SM3 algorithm of PF_KEY and convert "transform" to "PF_KEY ", add a SM3 array.

Table.2 Location of Mark

Mark	Location
transform	"include/ietf_constantsh";"Linux/include/openswan/ipsec_policy.h";"ipsec_xform.h"
PF_KEY	"Linux/include/pfkeyv2.h";
SPDB	"programs/Pluto/spdb.c"
Crypto	"programs/Pluto/crypto.c"

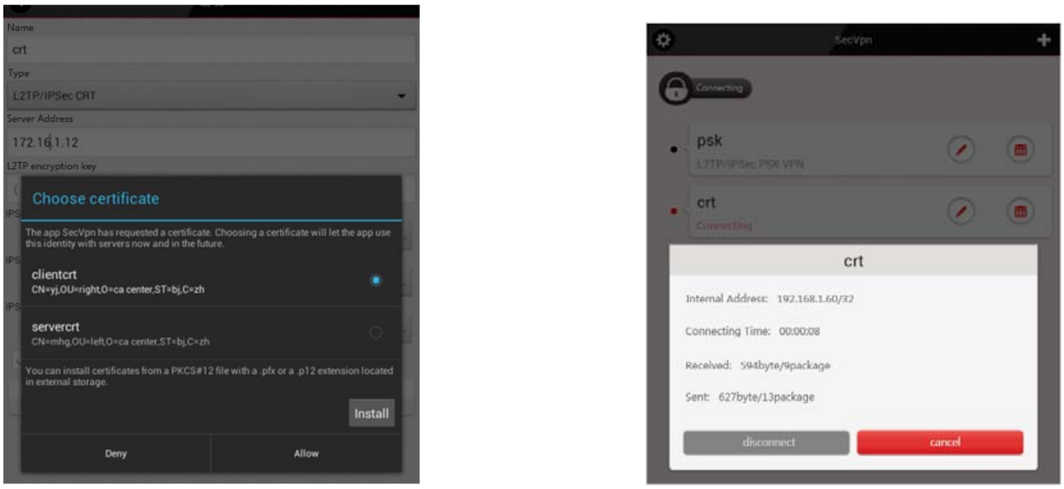
Result and Test of System Test Results

Tested the server of Ubuntu10.04, on which OpenSwan + x12tpdx built has been passed PSK and RSA model test, through the analysis IPSec – tools source code on the client software based on Android platform has realized the support of L2TP/IPSec PSK (Shared secret) connection, L2TP/IPSec connection of the CRT (certificate), p12 certificate of installation and analytical, boot automatically start, automatic connection, suspended window, and have the system logs, the VPN connection state monitoring mechanism, and other functions, test results are shown in figure 5. Tested the client through SDKEY password interface of this system can access security VPN successfully, connect to the server, and to protect the mobile terminals, data security, has the very high reliability and practicability.

The scheme has been tested on a Ubuntu10.04 server, the server depend on OpenSwan + x12tpdx that has been passed PSK and RSA model test through the analysis IPSec – tools' source code on the client software based on Android platform has realized, among others, the following functions:

- L2TP/IPSec PSK (Shared secret) connection,
- L2TP/IPSec connection of the CRT (certificate),
- P12 certificate of installation and analytical,
- Automatically booting,
- Automatic connection,
- Suspended window,
- And have the system logs, the
- VPN connection state monitoring mechanism

As shown in figure 5, the client, through SDKEY password interface of this system, can establish security VPN successfully, connect to the server, and protect mobile terminals. The new scheme demonstrated enhanced data security, high reliability, and usability in comparison to the existing systems.



Name: crt

Type: L2TP/IPSec CRT

Server Address: 172.16.1.12

L2TP encryption key

Choose certificate

The app SecVpn has requested a certificate. Choosing a certificate will let the app use this identity with servers now and in the future.

● clientcrt
CN=yj,OU=right,O=ca center,ST=bj,C=zh

○ servercrt
CN=mhg,OU=left,O=ca center,ST=bj,C=zh

You can install certificates from a PKCS#12 file with a .pfx or a .p12 extension located in external storage.

Internal Address: 192.168.1.60/32

Connecting Time: 00:00:08

Received: 594byte/9package

Sent: 627byte/13package

Fig.5 Test of the Client

Summary

Based on the investigation on IKE negotiation process and the study of the source code of various IPSec tools, the new security access system on mobile terminal based on IPSec VPN and encryption is proposed. The system succeeded to establish VPNs' between servers and mobile devices using IPSec. Therefore, the safety of the mobile device is guaranteed. The proposed system is safe and reliable, and able to solve problems of mobile terminal in data transmission, user identification, and application safety. It can be applied to practice to enhance the mobile device security access system nowadays.

References

[1] H. Yihao: Research and Improvement of IPSEC VPN Based On The Android System. (2012)

[2] C. Kaufman, P.Hoffan, Y. Nir, P. Eronen. RFC5996: Internet Key Exchange Protocol Version 2 [EB/OL]. IETF. (2010)

[3] X. Zhengrong, L. Yang: Study of network security access technology based on VPN. (2015)

[4] Singh, A.K. Samaddar, S.G: Enhancing VPN Security Through Security Policy Management. (2012)

[5] Park, Matthews: Characterizing the impacts of VPN security models on streaming video.(2010)