Khoa Khoa học & Kỹ thuật máy tính
Trường ĐH Bách Khoa TP.HCM

Cryptography and Network Security
Lab 7
Open VPN

INTRODUCTION

Virtual Private Network is a special network setup aimed to provide high level of confidentiality and integrity protection for data traffic exchanged between hosts or gateways. It is especially usefull in cases, when data transfer is carried out across the public Internet.

OpenVPN Access Server (https://openvpn.net/) is a full featured secure network tunneling VPN software solution that integrates OpenVPN server capabilities, enterprise management capabilities, simplified OpenVPN Connect UI, and OpenVPN Client software packages that accommodate Windows, MAC, and Linux OS environments. OpenVPN Access Server supports a wide range of configurations, including secure and granular remote access to internal network and/ or private cloud network resources and applications with fine-grained access control.

PRACTICE

1. First step: boot the computer in Windows. Create a new folder on the Desktop, for example “VPN”. Use it to store all files used throughout the lab.

2. Download OpenVPN from https://openvpn.net/index.php/open-source/downloads.html and install OpenVPN.

3. Use C:\Program Files\OpenVPN\easy-rsa to generate certificates, which will be used to set up secure VPN connection. Execute command: init-config. A new file

will appear: vars.bat. Edit the file to configure all parameters: KEY_COUNTRY, KEY_PROVINCE, KEY_CITY, KEY_ORG and KEY_EMAIL. Note that the file contains, among other things, the length of a key.

4. Create a new certificate authority with the following commands:

- vars
- clean-all
- build-ca

While executing the 'build-ca' command, you will be prompted to provide parameters previously defined in file vars.bat. It is enough just to confirm them. Nevertheless you must not forget to configure Common Name parameter to some value, for example to OpenVPN-CA.

5. Generate certificates and keys for the server:

- build-key-server server

Please use the phrase "server" as "Common Name" . Answer 'yes' to the questions: "Sign the certificate? [y/n] and "1 out of 1 certificate requests certified, commit? [y/n]"

6. Generate certificates and keys for 3 clients:

- build-key client1
- build-key client2
- build-key client3

Also this time you are advised to use a unique Common Name for each certificate (for exampe "client1", "client2" and "client3"). Otherwise certificates will not be generated in a proper way (file size: 0 bytes).

7. Parameters for key establishement have to be defined with the following command:

- build-dh

Please look into all fields that make up a certificate. (double click the certificate to open it). Below you can see all the files which have been generated up until this moment:

Filename	Needed By	Purpose	Secret
ca.crt	server + all clients	Root CA certificate	NO
ca.key	key signing machine only	Root CA key	YES
dh{n}.pem	server only	Diffie Hellman parameters	NO
server.crt	server only	Server Certificate	NO
server.key	server only	Server Key	YES
client1.crt	client1 only	Client1 Certificate	NO
client1.key	client1 only	Client1 Key	YES
client2.crt	client2 only	Client2 Certificate	NO
client2.key	client2 only	Client2 Key	YES
client3.crt	client3 only	Client3 Certificate	NO
client3.key	client3 only	Client3 Key	YES

a) Move the files to C:\Program Files\OpenVPN\config
b) Distribute some of these files to another group, which is maintaining the other end of the tunnel.
Q: which files should be distributed, and which files must not be distributed ?

PRACTICE

1. List and briefly describe some benefits of IPsec.
2. List and briefly define different categories of IPsec documents.
3. What parameters identify an SA and what parameters characterize the nature of a particular SA?
4. What is the difference between transport mode and tunnel mode?
5. What are the types of secret key algorithm used in IPsec?
6. Why does ESP include a padding field?
7. What are the basic approaches to bundling SAs?
8. What are the roles of the Oakley key determination protocol and ISAKMP in IPsec?
9. Where does IPsec reside in a protocol stack?
10. When tunnel mode is used, a new outer IP header is constructed. For both IPv4 and IPv6, indicate the relationship of each outer IP header field and each extension header in the outer packet to the corresponding field or extension header of the inner IP packet. That is, indicate which outer values are derived from inner values and which are constructed independently of the inner values.