Remote Access - what kind of security ?

Constantin Yamkoudougou, Security Consultant
email: security at itconstantin.com

24 novembre 2004

Introduction

The possibility of remotely using the resources of a local area network became essential for many companies. Such an access supposes the deployment within the local infrastructure of network of a set of equipments which enable the possibility to authenticate, allocate the resources according to the remote user profile. For certain companies specialized such as Internet services providers, accounting and on demand band-width management is essential to address the right invoicing to each customer who reaches Internet by the means of their network. There are many typologies of remote access protocols . There are early Internet protocols such as Telnet. SSH is the famous one of today. There are also the commonly so called light VPN such as PPTP, L2TP which are protocols of level 2 and finally the protocols more elaborate and complicated such as IPSec.

All these protocols do not offer the same level of security. Some do not offer any security at all such as Telnet. To control the remote access and to authenticate the users, the most known protocols with this intention is RADIUS which evolved in DIAMETER. TACACS also shoud not be forbidden when talking about remote authentication.

Remote acess over RADIUS protocol

RADIUS (Remote Authentication Dial In Using Services) has a client /server architecture. The TCP ports dedicated to the server by the IANA are 1812 for the process of authentification and the port 1813 for accounting and billing. DIAMETER is a protocol that inherits the main characteristics of RADIUS while it uses UDP as a transport protocol. A reproach made to RADIUS and DIAMETER is to ensure no data confidentiality between the remote stations seeking the client for an authentication (RADIUS/DIAMETER). This confidentiality is only ensured between the client and RADIUS/DIAMETER server. In the process of authentication of the remote station to the local network RADIUS client, the most common used protocols are PAP (Password Authentication Protocol) or another one by

challenge/response which is CHAP on the port 1723.

Remote access over TELNET

Another alternative of remote access protocol is TELNET. TELNET is an Internet remote access protocol of first generation. It allows a remote user to be connected on a computer by using a login and a password in the process of identification and authentification. The user then has a shell to type and execute command lines. The user seems to be connected locally to the distant machine. Unfortunately this protocol offers only a very little security. The login and the password are transmitted in clear text mode on Internet et nothing is ciphered. Today, it is recommended to use more elaborate protocol such as SSH which offers a better security than TELNET.

Remote authentication over PPTP

PPTP (Point To Point Tunneling Protocol) is usually used on access network of PSTN. PPTP is an extension of PPP protocol designed by Microsoft. Architectures using this type of technology generally involve three computers : a client, an access server an the PPTP server. The PPTP client is typically installed on the client PC . The second computer involved is the network access server (NAS) which is located at the border of the distant network. The client uses PPP to get connected to the NAS server. Once this connection is established a second connection uses PPTP protocol over PPP to be connected to the PPTP server. Then PPTP acts as a VPN or a tunnel for future data transfer. Data transfer between the access serveur and the client PC is not secured. But PPTP enables optionally data encryption between the user PC and the PPTP server. PPTP is usefull to provide a roaming to ISP's customers. Let's say that your ISP have a PPTP server and has concluded agreements with many other operators. Because your ISP server is known by the other operators' NAS, you will be able to authenticate yourself through the PPTP to your home authentication server.

Remote acess over L2TP

L2TP has the same futures as PPTP and was originally designed and submitted by Cisco for the purposes of an extension of L2F protocol. This protocol has the same functionalities as PPTP except that it has been created to take into account of large diversity of networks : ATM, frame relay, whereas PPTP supports only IP. This protocol uses UDP port 1701 and was dedicated to hardware implementation primarily. It is compatible with the majority of existing AAA servers ie RADIUS, DIAMATER and TACACS+

Remote access - is IPSEC or SSL suitable ?

To create a similar environment to this one the user has in his daily computer desktop space at office, IPSec is the most popular used protocol because of the security layer it provides. But IPSEC is more and more criti-

cized because of its complicated keys management system, specific getways deployment. Moreover the user in motion or working remotely at home is attached to a given laptop or a computer where there could be confidential business informations stored on it. It could be a real concern if such a laptop or remote workstation is stolen or compromised. All these criticisms arose a new concept on working remotely with SSL now preferred to IPSec. Todays some start-ups offer services giving access to any busines application via SSL. It's only necessary to get a brower installed on any PC. The remote user just load a secured java applet and can do everything he does with a classical IPsec network connection. No matter the remote worker is connected on a public computer or not because all he does depend on the SSL session. IPsec is no longer the de facto tool to think about when you have to implement a VPN for remote work.