

Forum:[Hack Forums](#)

Thread: [What is a PPTP VPN](#)

ihacktolearn - November 1, 2010, 8:56 pm

Can somebody explain what a PPTP VPN is, i know what a VPN is just not a PPTP, what does a PPTP VPN do and how does it work?

Ryzaar - November 2, 2010, 2:31 am

http://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol

After a short skim read, I assume it's similar to a VPN but less secure as far as encryption and logging go.

Again, just an assumption, I didn't read it extensively- but that's the impression I got from the first paragraph

EDIT I noticed a section to do with security.

Quote:PPTP has been the subject of many security analyses and serious security vulnerabilities have been found in the protocol. The known vulnerabilities relate to the underlying PPP authentication protocols used, the design of the MPPE protocol as well as the integration between MPPE and PPP authentication for session key establishment. A summary of these vulnerabilities is below:

MSCHAP-v1 is fundamentally insecure. Tools exist to trivially extract the NT Password hashes from a captured MSCHAP-v1 exchange.[3]

MSCHAP-v2 is vulnerable to dictionary attack on the captured challenge response packets. Tools exist to perform this process rapidly. [1]

When using MSCHAP-v1, MPPE uses the same RC4 session key for encryption in both directions of the communication flow. This can be cryptanalysed with standard methods by XORing the streams from each direction together.[4]

MPPE uses RC4 stream cipher for encryption. There is no method for authentication of the ciphertext stream and therefore the ciphertext is vulnerable to a bit-flipping attack. An attacker could modify the stream in transit and adjust single bits to change the output stream without possibility of detection. These bit flips may be detected by the protocols themselves through checksums or other means.[5]

EAP-TLS is seen as the superior authentication choice for PPTP [2]; however, it requires implementation of a Public Key Infrastructure for both client and server certificates. As such it is not a viable authentication option for many remote access installations

So yes, just a very insecure version of a VPN