

PV204: Assignment #04

Peter Kotvan

VPN vs. Wi-Fi

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. [1]

Wi-Fi security

For encryption, the only difference between WPA and WPA2 is that WPA2 mandates both TKIP (a proper implementation of RC4) and AES encryption (good enough for top secret government security), whereas WPA mandated only TKIP encryption with optional AES support. Neither TKIP or AES is considered broken, though AES is unquestionably superior.

WPA/WPA2 has two modes of authentication and access control: home PSK mode and enterprise 802.1x mode. For home mode, the use of multiple rounds of hashing makes dictionary attacks painfully slow and the implementation of a "salt" in the key rules out the use of pre-computed hash tables (unless attacking a common SSID). The enterprise mode of WPA calls for 802.1x, which is a standard for port-based network access control that is open to a wide range of EAP (Extensible Authentication Protocol) types. The stronger EAP types, like EAP-TLS, PEAP, or EAP-TTLS, use PKI digital certificates for strong authentication. Weaker EAP types, such as Cisco LEAP, transmit hashed passwords in the clear and are easy to crack with dictionary attacks. Other weak implementations, like Cisco EAP-FAST, are typically deployed with anonymous digital certificates, which make them almost as easy to attack as LEAP. [2]

VPN security

VPN is a privacy technology where the encryption usually happens at the network layer (Layer 3 of the OSI model) with technology such as IPSEC, PPTP, and L2TP. More recent VPN implementations have moved to SSL tunneling for ease of firewall, NAT, and proxy traversal (bypass) where the encryption happens at the presentation layer (Layer 6 of the OSI model). Note that most VPN solutions emulate a Layer 2 connection by encapsulating Layer 2 within Layer 3 IPSEC or Layer 6 SSL. Layer 2 emulation allows the VPN client to have a virtual IP address on the remote LAN it's connecting to. Some SSL-tunneling VPN (not to be confused with application layer SSL-VPN) vendors, like Cisco, use ActiveX and/or Java installers to make it possible to rapidly deploy the VPN client from a Web-based install. Microsoft will soon begin to incorporate a new SSL-tunneling technology, called SSTP, into Windows' built-in VPN client, which currently supports only PPTP and L2TP.

Encryption and authentication used in VPN vary depending on the implementation. Implementations such as PPTP VPN use RC4 (40-, 56-, and 128-bit), whereas IPSEC and L2TP can use a wide range of encryption algorithms, like DES (56-bit), 3DES (168-bit), and AES (128-, 192-, and 256-bit). Authentication mechanisms in VPN can be weak, like PPTP, which transmits hashed passwords in the clear, or they can be strong PKI-based implementations, like L2TP, which uses server and client digital certificates. Some IPSEC

solutions will have the option of using a pre-shared key or PKI-based digital certificates. If this sounds a lot like Wi-Fi security above, it's not your imagination – the principles of cryptography are universal. [2]

SSH Tunneling

A secure shell (SSH) tunnel consists of an encrypted tunnel created through an SSH protocol connection. Users may set up SSH tunnels to transfer unencrypted traffic over a network through an encrypted channel. [3]

SSH tunnels can be created in several ways using different kinds of port forwarding mechanisms. Openssh can forward ports in three ways.

Local port forwarding

Flag -L specifies that the given port on the local (client) host is to be forwarded to the given host and port on the remote side. This works by allocating a socket to listen to port on the local side, optionally bound to the specified bind address. Whenever a connection is made to this port, the connection is forwarded over the secure channel, and a connection is made to host port hostport from the remote machine.

Remote port forwarding

Flag -R specifies that the given port on the remote (server) host is to be forwarded to the given host and port on the local side. This works by allocating a socket to listen to port on the remote side, and whenever a connection is made to this port, the connection is forwarded over the secure channel, and a connection is made to host port hostport from the local machine.

Dynamic port forwarding

Flag -D specifies a local *dynamic* application-level port forwarding. This works by allocating a socket to listen to port on the local side, optionally bound to the specified bind address. Whenever a connection is made to this port, the connection is forwarded over the secure channel, and the application protocol is then used to determine where to connect to from the remote machine. Currently the SOCKS4 and SOCKS5 protocols are supported, and ssh will act as a SOCKS server.'

[4]

References

- [1] Wikipedia. *Virtual private network*. 2014. URL: https://en.wikipedia.org/wiki/Virtual_Private_Network.
- [2] George Ou. *Why VPN can't replace Wi-Fi security*. URL: <http://www.zdnet.com/blog/ou/why-vpn-cant-replace-wi-fi-security/489>.
- [3] Wikipedia. *Tunneling protocol*. 2014. URL: https://en.wikipedia.org/wiki/Tunneling_protocol.
- [4] *Openssh manual page*. openssh v6.6. 2014.