WIKIPEDIA

Point-to-Point Tunneling Protocol

The **Point-to-Point Tunneling Protocol** (**PPTP**) is an obsolete method for implementing virtual private networks. PPTP has many well known security issues.

PPTP uses a TCP control channel and a Generic Routing Encapsulation tunnel to encapsulate PPP packets. Many modern VPNs use various forms of UDP for this same functionality.

The PPTP specification does not describe encryption or authentication features and relies on the Point-to-Point Protocol being tunneled to implement any and all security functionalities.

The PPTP implementation that ships with the Microsoft Windows product families implements various levels of authentication and encryption natively as standard features of the Windows PPTP stack. The intended use of this protocol is to provide security levels and remote access levels comparable with typical VPN products.

Contents

History

A specification for PPTP was published in July 1999 as RFC 2637[1] and was developed by a vendor consortium formed by Microsoft, Ascend Communications (today part of Nokia), 3Com, and others.

PPTP has not been proposed nor ratified as a standard by the Internet Engineering Task Force.

Description

A PPTP tunnel is instantiated by communication to the peer on TCP port 1723. This TCP connection is then used to initiate and manage a GRE tunnel to the same peer. The PPTP GRE packet format is non standard, including a new *acknowledgement number* field replacing the typical *routing* field in the GRE header. However, as in a normal GRE connection, those modified GRE packets are directly encapsulated into IP packets, and seen as IP protocol number 47. The GRE tunnel is used to carry encapsulated PPP packets, allowing the tunnelling of any protocols that can be carried within PPP, including IP, NetBEUI and IPX.

In the Microsoft implementation, the tunneled PPP traffic can be authenticated with PAP, CHAP, MS-CHAP v1/v2 .

Security

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.[2][3][4][5]

A summary of these vulnerabilities is below:

- MS-CHAP-v1 is fundamentally insecure. Tools exist to trivially extract the NT Password hashes from a captured MSCHAP-v1 exchange.[6]
- When using MS-CHAP-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.[7]
- MS-CHAP-v2 is vulnerable to dictionary attacks on the captured challenge response packets. Tools exist to perform this process rapidly.[8]
- In 2012, it was demonstrated that the complexity of a brute-force attack on a MS-CHAP-v2 key is equivalent to a brute-force attack on a single DES key. An online service was also demonstrated which is capable of decrypting a MS-CHAP-v2 MD4 passphrase in 23 hours.[9][10]
- MPPE uses the 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.[6]

EAP-TLS is seen as the superior authentication choice for PPTP;[11] however, it requires implementation of a public-key infrastructure for both client and server certificates. As such, it may not be a viable authentication option for some remote access installations. Most networks that use PPTP have to apply additional security measures or be deemed completely inappropriate for the modern internet environment. At the same time, doing so means negating the aforementioned benefits of the protocol to some point.[12]

See also

- IPsec
- Layer 2 Tunneling Protocol (L2TP)
- Secure Socket Tunneling Protocol (SSTP)
- OpenVPN, open source software application that implements VPN
- WireGuard, a simple and effective VPN implementation

References

1. RFC 2637
2. "Malware FAQ: Microsoft PPTP VPN" (https://www.sans.org/security-resources/malwarefaq/pptp-vpn). Retrieved 2017-06-29.
3. "Microsoft says don't use PPTP and MS-CHAP" (http://www.h-online.com/security/news/item/Microsoft-says-don-t-use-PPTP-and-MS-CHAP-1672257.html). Retrieved 2012-11-03.
4. "A death blow for PPTP" (http://www.h-online.com/security/features/A-death-blow-for-PPTP-1716768.html). Retrieved 2012-11-03.

5. "Differences between PPTP and L2TP" (https://web.archive.org/web/20160914125558/https://www.bestvpnrating.com/blog/main-differences-between-pptp-l2tp). *bestvpnrating*. Archived from the original (https://www.bestvpnrating.com/blog/main-differences-between-pptp-l2tp) on 14 September 2016. Retrieved 7 August 2016.
6. Bruce Schneier, *Cryptanalysis of Microsoft's Point to Point Tunneling Protocol (PPTP)* (http://www.schneier.com/paper-pptp.pdf).
7. Bruce Schneier, *Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)*, October 19 1999 (http://www.schneier.com/paper-pptpv2.pdf).
8. Wright, Joshua. "Asleap" (http://www.willhackforsushi.com/?page_id=41). Retrieved 2017-11-01.
9. "Divide and Conquer: Cracking MS-CHAPv2 with a 100% success rate" (https://web.archive.org/web/20160316174007/https://www.cloudcracker.com/blog/2012/07/29/cracking-ms-chap-v2/). Cloudcracker.com. 2012-07-29. Archived from the original (https://www.cloudcracker.com/blog/2012/07/29/cracking-ms-chap-v2/) on 2016-03-16. Retrieved 2012-09-07.
10. "Marlinspike demos MS-CHAPv2 crack" (https://www.theregister.co.uk/2012/07/31/ms_chapv2_crack/). The Register. 2012-07-31. Retrieved 2012-09-07.
11. Choosing (https://technet.microsoft.com/en-us/library/cc739638%28WS.10%29.aspx)EAP-TLS or MS-CHAP v2 for User-Level Authentication, Microsoft TechNet, March 28, 2003
12. "VPN Protocol Comparison: IKEv2 vs IKEv1 vs OpenVPN vs L2TP vs PPTP" (https://www.vpnunlimitedapp.com/blog/vpn-protocol-comparison/). *VPN Unlimited Blog*. 2018-05-14. Retrieved 2018-06-19.

External links

- Windows NT: Understanding PPTP (http://www.microsoft.com/technet/archive/winntas/plan/pptpudst.mspx) from Microsoft
- FAQ on security flaws in Microsoft's implementation (http://www.schneier.com/pptp-faq.html), Bruce Schneier, 1998
- Cryptanalysis of Microsoft's PPTP Authentication Extensions (http://www.schneier.com/paper-pptpv2.html) (MS-CHAPv2), Bruce Schneier, 1999

Retrieved from "https://en.wikipedia.org/w/index.php?title=Point-to-Point_Tunneling_Protocol&oldid=1001114472"

This page was last edited on 18 January 2021, at 09:02 (UTC).