Cryptology ePrint Archive: Report 2011/284

On the Security of PPPoE Network

Fanbao Liu and Yumeng Feng and Yuan Cao

Abstract: PPPoE is a network protocol for encapsulating PPP frames inside Ethernet. It is widely used by commercial ISPs to authenticate peers, who want to surf the Internet by paying the bills. In this paper, we analyze the security of the PPPoE network, we find that we can easily collect information about both the peers and the PPPoE authentication servers. We can use such information to recover the peer's authentication password by silently impersonating the server, which is undetectable in the network. We impersonate the server in the peers' LAN and get their passwords by hijacking the peers' PPPoE connections and negotiating for using the PAP authentication protocol. We further propose an efficient password recovery attack against the CHAP authentication protocol. We first recover the length of the password through on-line queries, based on the weakness of MD5 input pre-processing. Then we crack the known length password off-line, using the probabilistic context-free grammars. For MS-CHAP has already been proved to be weak, and the more secure EAP authentication methods can be by-passed through roll-back attack, which negotiates the weak protocols, the authentication passwords of the PPPoE networks are truly in danger. We point out that PPPoE can't be used any more, until all of the weak authentication protocols including PAP, CHAP, MS-CHAP are abolished right now and replaced with more secure EAP methods.

Category / Keywords: PPPoE, Authentication Protocol, Password Recovery, PPP, PAP, CHAP.

Date: received 30 May 2011

Contact author: liufanbao at gmail com

Available formats: PDF | BibTeX Citation

Version: 20110603:150129 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]