                       PPP Authentication Protocols

Status of this Memo

   This RFC specifies an IAB standards track protocol for the Internet
   community, and requests discussion and suggestions for improvements.
   Please refer to the current edition of the "IAB Official Protocol
   Standards" for the standardization state and status of this protocol.
   Distribution of this memo is unlimited.

Abstract

   The Point-to-Point Protocol (PPP) [1] provides a standard method of
   encapsulating Network Layer protocol information over point-to-point
   links. PPP also defines an extensible Link Control Protocol, which
   allows negotiation of an Authentication Protocol for authenticating
   its peer before allowing Network Layer protocols to transmit over the
   link.

   This document defines two protocols for Authentication: the Password
   Authentication Protocol and the Challenge-Handshake Authentication
   Protocol. This memo is the product of the Point-to-Point Protocol
   Working Group of the Internet Engineering Task Force (IETF).
   Comments on this memo should be submitted to the ietf-ppp@ucdavis.edu
   mailing list.

Table of Contents

1. Introduction

      PPP has three main components:

         1. A method for encapsulating datagrams over serial links.

         2. A Link Control Protocol (LCP) for establishing, configuring,
            and testing the data-link connection.

         3. A family of Network Control Protocols (NCPs) for establishing
            and configuring different network-layer protocols.

      In order to establish communications over a point-to-point link, each
      end of the PPP link must first send LCP packets to configure the data
      link during Link Establishment phase. After the link has been
      established, PPP provides for an optional Authentication phase before
      proceeding to the Network-Layer Protocol phase.

      By default, authentication is not mandatory. If authentication of
      the link is desired, an implementation MUST specify the
      Authentication-Protocol Configuration Option during Link
      Establishment phase.

      These authentication protocols are intended for use primarily by
      hosts and routers that connect to a PPP network server via switched
      circuits or dial-up lines, but might be applied to dedicated links as
      well. The server can use the identification of the connecting host
      or router in the selection of options for network layer negotiations.

      This document defines the PPP authentication protocols. The Link
      Establishment and Authentication phases, and the Authentication-
      Protocol Configuration Option, are defined in The Point-to-Point
      Protocol (PPP) [1].

1.1. Specification Requirements

      In this document, several words are used to signify the requirements
      of the specification. These words are often capitalized.

      MUST
         This word, or the adjective "required", means that the definition
         is an absolute requirement of the specification.

MUST NOT
   This phrase means that the definition is an absolute prohibition
   of the specification.

SHOULD
   This word, or the adjective "recommended", means that there may
   exist valid reasons in particular circumstances to ignore this
   item, but the full implications should be understood and carefully
   weighed before choosing a different course.

MAY
   This word, or the adjective "optional", means that this item is
   one of an allowed set of alternatives. An implementation which
   does not include this option MUST be prepared to interoperate with
   another implementation which does include the option.

1.2. Terminology

   This document frequently uses the following terms:

   authenticator
      The end of the link requiring the authentication. The
      authenticator specifies the authentication protocol to be used in
      the Configure-Request during Link Establishment phase.

   peer
      The other end of the point-to-point link; the end which is being
      authenticated by the authenticator.

   silently discard
      This means the implementation discards the packet without further
      processing. The implementation SHOULD provide the capability of
      logging the error, including the contents of the silently
      discarded packet, and SHOULD record the event in a statistics
      counter.

2. Password Authentication Protocol

   The Password Authentication Protocol (PAP) provides a simple method
   for the peer to establish its identity using a 2-way handshake. This
   is done only upon initial link establishment.

   After the Link Establishment phase is complete, an Id/Password pair
   is repeatedly sent by the peer to the authenticator until
   authentication is acknowledged or the connection is terminated.

   PAP is not a strong authentication method. Passwords are sent over
   the circuit "in the clear", and there is no protection from playback

or repeated trial and error attacks. The peer is in control of the
frequency and timing of the attempts.

Any implementations which include a stronger authentication method
(such as CHAP, described below) MUST offer to negotiate that method
prior to PAP.

This authentication method is most appropriately used where a
plaintext password must be available to simulate a login at a remote
host. In such use, this method provides a similar level of security
to the usual user login at the remote host.

   Implementation Note: It is possible to limit the exposure of the
   plaintext password to transmission over the PPP link, and avoid
   sending the plaintext password over the entire network. When the
   remote host password is kept as a one-way transformed value, and
   the algorithm for the transform function is implemented in the
   local server, the plaintext password SHOULD be locally transformed
   before comparison with the transformed password from the remote
   host.

2.1. Configuration Option Format

A summary of the Authentication-Protocol Configuration Option format
to negotiate the Password Authentication Protocol is shown below.
The fields are transmitted from left to right.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |     Authentication-Protocol    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
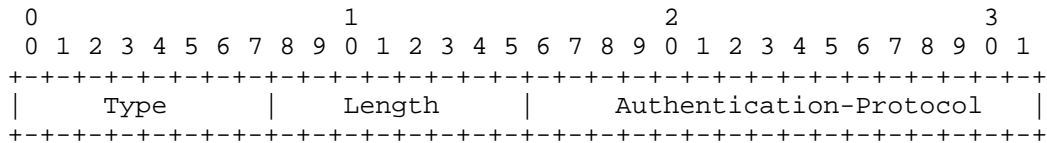
Type

   3

Length

   4

Authentication-Protocol

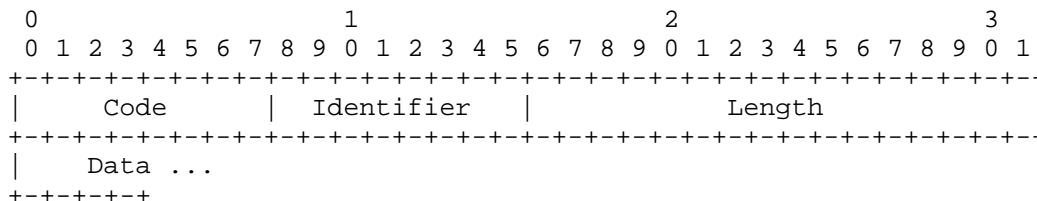   c023 (hex) for Password Authentication Protocol.

Data

   There is no Data field.

Lloyd & Simpson   [Page 4]

2.2. Packet Format

   Exactly one Password Authentication Protocol packet is encapsulated
   in the Information field of a PPP Data Link Layer frame where the
   protocol field indicates type hex c023 (Password Authentication
   Protocol). A summary of the PAP packet format is shown below. The
   fields are transmitted from left to right.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Code      |  Identifier   |            Length             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |    Data ...
   +-+-+-+-+
```

   Code

      The Code field is one octet and identifies the type of PAP packet.
      PAP Codes are assigned as follows:

         1   Authenticate-Request
         2   Authenticate-Ack
         3   Authenticate-Nak

   Identifier

      The Identifier field is one octet and aids in matching requests
      and replies.

   Length

      The Length field is two octets and indicates the length of the PAP
      packet including the Code, Identifier, Length and Data fields.
      Octets outside the range of the Length field should be treated as
      Data Link Layer padding and should be ignored on reception.

   Data

      The Data field is zero or more octets. The format of the Data
      field is determined by the Code field.

2.2.1. Authenticate-Request

   Description

      The Authenticate-Request packet is used to begin the Password
      Authentication Protocol. The link peer MUST transmit a PAP packet

Lloyd & Simpson   [Page 5]

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.

fastcase®
Smarter legal research.