Network Security

Chapter 10

Security Protocols of the Data Link Layer

- IEEE 802.1x
- Point-to-Point Protocol (PPP)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- Virtual Private Networks (VPN)
Scope of Link Layer Security Protocols

- According to the classical understanding of the OSI model, the link layer provides an assured data transmission service *between two peer entities that are directly inter-connected by a communications medium*.

- Its main tasks are:
  - Error detection and correction
  - Medium access control (MAC, not to be mixed up with message authentication code) for shared media, e.g. Ethernet, etc.

- Not all of today’s networking technology fits nicely into that model:
  - Dial-up connections to an Internet service provider
  - Virtual Private Network (VPN) solutions

- In this class, we content ourselves with the following definition:
  - The purpose of a link layer security protocol is to ensure specific security properties of link layer PDUs, that is the PDUs of the protocol layer carrying the PDUs of the network layer (e.g. IP)
IEEE 802.1x: Background & Goals

- The Institute of Electrical and Electronics Engineers (IEEE) 802 LAN/MAN Standards Committee develops local area network standards and metropolitan area network standards.

- The most widely used standards are:
  - Ethernet family (802.3, generally referred to as CSMA/CD),
  - Token Ring (802.5),
  - Wireless LAN (802.11)

- The IEEE committee is currently working on a standard that:
  - aims to “restrict access to the services offered by a LAN to those users and devices that are permitted to make use of those services”
  - may be used with different IEEE 802.x technologies
  - defines port based network access control to provide a means of “ authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics”
  - is generally referred to as IEEE 802.1x
IEEE 802.1x introduces the notion of two logical ports:
- the uncontrolled port allows to authenticate a device
- the controlled port allows an authenticated device to access LAN services
IEEE 802.1x: Roles

- Three principal roles are distinguished:
  - A device that wants to use the service offered by an IEEE 802.1x LAN acts as a *supplicant* requesting access to the controlled port.
  - The point of attachment to the LAN infrastructure (e.g. a MAC bridge) acts as the *authenticator* demanding the supplicant to authenticate itself.
  - The authenticator does not check the credentials presented by the supplicant itself, but passes them to his *authentication server* for verification.

- Accessing a LAN with IEEE 802.1x security measures:
  - Prior to successful authentication the supplicant can access the uncontrolled port:
    - The port is uncontrolled in the sense, that it allows access prior to authentication.
    - However, this port allows only restricted access.
  - Authentication can be initiated by the supplicant or the authenticator.
  - After successful authentication the controlled port is opened.
IEEE 802.1x Security Protocols & Message Exchange

- IEEE 802.1x does not define its own security protocols, but advocates the use of existing protocols:
  - The Extensible Authentication Protocol (EAP) may realize basic device authentication [RFC 2284]
  - If negotiation of a session key during authentication is required, the use of the PPP EAP TLS Authentication Protocol is recommended [RFC 2716]
  - Furthermore, the authentication server is recommended to be realized with the Remote Authentication Dial In User Service (RADIUS) [RFC 2865]
- Exchange of EAP messages between supplicant and authenticator is realized with the EAP over LANs (EAPOL) protocol:
  - EAPOL defines the encapsulation techniques that shall be used in order to carry EAP packets between supplicant port access entities (PAE) and Authenticator PAEs in a LAN environment
  - EAPOL frame formats have been defined for various members of the 802.x protocol family, e.g. EAPOL for Ethernet, ...
  - Between supplicant and authenticator RADIUS messages may be used
IEEE 802.1x: Example of an 802.1x Authentication

<table>
<thead>
<tr>
<th>Supplicant PAE</th>
<th>Authenticator PAE</th>
<th>Authentication Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAPOL-Start</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>EAP-Request/Identity</td>
</tr>
<tr>
<td>EAP-Response/Identity(MyID)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>EAP-Request/OTP OTP Challenge</td>
</tr>
<tr>
<td>EAP-Request/OTP OTP Passwd</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>EAP-Success</td>
</tr>
<tr>
<td>Authentication successfully completed</td>
<td>Port authorized</td>
<td>[source: IEEE Draft P802.1X/D11]</td>
</tr>
</tbody>
</table>
Point-to-Point Protocol: Purpose and Tasks

- Large parts of the Internet rely on point-to-point connections:
  - Wide area network (WAN) connections between routers
  - Dial-up connections of hosts using modems and telephone lines

- Protocols for this purpose:
  - Serial Line IP (SLIP): no error detection, supports only IP, no dynamic address assignment, no authentication [RFC 1055]
  - Point-to-Point Protocol (PPP): successor to SLIP, supports IP, IPX, ...

- PPP [RFC 1661/1662]:
  - Layer-2 frame format with frame delimitation and error detection
  - Control protocol (Link Control Protocol, LCP) for connection establishment, -test, -negotiation, and -release
  - Separate Network Control Protocols (NCP) for supported Layer-3 protocols
Point-to-Point Protocol: Packet Format

- Character-oriented (instead of bit-oriented) ⇒ byte aligned frames
- Code transparency achieved through character stuffing
- Usually only unnumbered frames are transmitted, however, in scenarios with high error probability (wireless communications) a more reliable mode with sequence numbers and re-transmissions can be negotiated
- Supported protocols for the payload field are, among others: IP, IPX, Appletalk
- If not otherwise negotiated the maximum payload size is 1500 byte
- Additional negotiation supports smaller packet headers
Point-to-Point Protocol: A Typical PPP Connection

- **Usage Scenario “Internet access of a PC via modem”:**
  - User calls *Internet service provider (ISP)* via modem and establishes a “physical” connection via the plain old telephone service (POTS)
  - Caller sends multiple LCP-packets in PPP-frames to chose desired PPP-parameters
  - Security specific negotiation (see below)
  - Exchange of NCP-packets to configure network layer:
    - e.g. configuration of IP including dynamic allocation of an IP address via Dynamic Host Configuration Protocol (DHCP)
  - Caller may use arbitrary Internet services like any other host with a fixed connection to the Internet
  - For connection termination the allocated IP address and the network layer connection are released
  - The layer-2 connection is released via LCP and the modem closes down the “physical” connection
Frame format of the Link Control Protocol (LCP):

- **Code**: configure-request, configure-ack, configure-nack, configure-reject, terminate-request, terminate-ack, code-reject, protocol-reject, echo-request, echo-reply, discard-request
- **Length**: indicates the length of the LCP-packet including the code field etc.
- **Data**: zero or more octets of command-specific data

The `configure` primitives of LCP allow to configure the link layer:

- There exist various options for this primitive for configuration of different aspects (max. receive unit, protocol compression, authentication, ...)

---

The original version of PPP [RFC 1661] suggests the optional run of an authentication protocol after the link establishment phase:

- If required, authentication is demanded by one peer entity via an LCP Configuration-Request at the end of the link establishment phase

- Originally, two authentication protocols have been defined:
  - Password Authentication Protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)

- Meanwhile, an extensible protocol has been defined:
  - Extensible Authentication Protocol (EAP)
  - PPP EAP Transport Level Security Protocol (PPP-EAP-TLS)

Furthermore, encryption can be negotiated after authentication:

- Protocols:
  - Encryption Control Protocol (ECP) for negotiation
  - PPP DES Encryption Protocol (DESE)
  - PPP Triple DES Encryption Protocol (3DESE)
Password Authentication Protocol (PAP):

- PAP was defined 1992 in RFC 1334
- The protocol is very simple:
  - Prerequisite: the authenticator knows a password of the peer entity
  - At the end of the link establishment phase one entity, called authenticator, demands the peer entity to authenticate with PAP
  - The peer entity sends an authenticate-request message containing its’ peer ID and password
  - The authenticator checks if the provided information is correct and answers with either an authenticate-ack or an authenticate-nack
- As the protocol provides no cryptographic protection, it is insecure
- PAP is not mentioned in updated RFCs for PPP authentication [RFC1994]
Point-to-Point Protocol: Authentication Protocols (2)

- Challenge Handshake Authentication Protocol (CHAP):
  - CHAP is also defined in RFC 1334 and RFC 1994
  - It realizes a simple challenge-response protocol:
    - Prerequisite: authenticator and peer entity share a secret
    - After the link establishment phase the authenticator (A) sends a challenge message containing an identifier for this challenge, a random number \( r_A \), and its name to the peer entity (B):
      \[
      A \rightarrow B: (1, \text{identifier}, r_A, A)
      \]
    - The peer entity computes a cryptographic hash function over its name, the shared secret \( K_{A,B} \) and the challenge random number \( r_A \) and sends the following message:
      \[
      B \rightarrow A: (2, \text{identifier}, H(B, K_{A,B}, r_A), B)
      \]
    - Upon reception of this message the authenticator re-computes the hash value and compares it with the received one; if both values match it answers with a success message
    - RFC 1994 specifies, that MD5 must be supported as hash function, but use of other hash functions can be negotiated
### CHAP message format:

- **Code**: 1 ~ challenge / 2 ~ response
- **Identifier**: one octet that has to be changed with every challenge sent
- **Length**: the overall length of the CHAP message in octets
- **Value Size**: one octet indicating the length of the value
- **Value**: contains the random challenge / the response to the challenge
- **Name**: one or more octets identifying the system that created the packet, the size of the name is calculated using the length field
## Point-to-Point Protocol: Authentication Protocols (4)

### CHAP message format:
- **Code**: 3 ~ success / 4 ~ failure
- **Identifier**: one octet that has to be changed with every challenge sent
- **Length**: the overall length of the CHAP message in octets
- **Message**:
  - Zero or more octets with implementation-dependent content
  - Its content is supposed to be human readable and has no influence on the operation of the protocol

<table>
<thead>
<tr>
<th>Code</th>
<th>Identifier</th>
<th>Length</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>02</td>
<td>3</td>
<td>15</td>
<td>1573 1</td>
</tr>
</tbody>
</table>
Point-to-Point Protocol: Authentication Protocols (5)

- Extensible Authentication Protocol (EAP):
  - EAP is a general protocol for PPP authentication which supports multiple authentication methods [RFC2284]
  - The main idea behind EAP is to provide a common protocol to run more elaborate authentication methods than “1 question + 1 answer”
  - The protocol provides basic primitives:
    - Request, Response: further refined by type field + type specific data
    - Success, Failure: to indicate the result of an authentication exchange
  - Type fields:
    - Identity
    - Notify
    - Nak (response only, to answer unacceptable request types)
    - MD5 Challenge (this corresponds to CHAP)
    - One-Time Password (OTP): defined in [RFC2289]
    - Generic Token Card
    - EAP-TLS
One-Time Password (OTP):

- The basic idea of OTP is to transmit a “password”, that can only be used for one run of an authentication dialogue.

Initial Setup:

- The authenticator $A$ sends a seed value $r_A$ and the peer entity $B$ concatenates it with his password and computes a hash value: $PW_N = H^N(r_A, \text{password}_B)$.
- The pair $(N, PW_N)$ is “securely” transmitted to the authenticator and stored at the authenticator.

Authentication dialogue:

- $A \rightarrow B$: $N - 1$
- $B \rightarrow A$: $PW_{N-1} := H^{N-1}(r_A, \text{password}_B)$
- $A$ checks if $H(PW_{N-1}) = PW_N$, and stores $(N - 1, PW_{N-1})$ as the new authentication information for $B$.

Security: In order to break this scheme, an attacker would have to eavesdrop one $PW_N$ and compute $H^{-1}(PW_N)$ which is impractical.
Generic Token Card:
- Basically, a challenge response dialogue
- A token card is used to compute a response to a challenge:
  - The challenge is presented to the user who has to type it to his token card device
  - The token card computes and displays the response
  - The user enters the response into the system that sends it as an answer to the challenge message

PPP-EAP-TLS:
- TLS stands for Transport Layer Security [RFC 2246]
- Thus, the authentication dialogue of TLS is run
- This dialogue will be explained in detail in chapter 12 on transport layer security
Point-to-Point Protocol: Encryption Protocols (1)

- After the link establishment and the authentication phase, encryption can be negotiated for a PPP connection:
  - The *Encryption Control Protocol (ECP)* [RFC1968] is responsible for configuring and enabling data encryption algorithms on both ends of the PPP link:
    - ECP uses the same frame format as LCP and introduces two new primitives: Reset-Request and Reset-Ack for indicating decryption errors independently for each direction (useful for cryptographic resynchronization)
    - A specific encryption method is negotiated using the `configure` primitive containing an option specifying *DESE, 3DESE, Proprietary*, etc.
    - Proprietary encryption protocols are identified by a registered *organizational unit identifier (OUI) + a vendor specific value*
    - Exactly one ECP packet is transported in the PPP information field of a link layer packet
    - ECP packets are identified by the PPP protocol field:
      - 0x8053 for “standard” operation
      - 0x8055 for individual link data encryption on multiple links to the same destination
The PPP DES Encryption Protocol (DESE):

This class will discuss only the updated version DESEv2 [RFC2419]

<table>
<thead>
<tr>
<th>Code</th>
<th>Identifier</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Length’</td>
<td>Initial Nonce</td>
</tr>
</tbody>
</table>

DESEv2 is negotiated with an ECP configure request message:

- **Code**: 1 ~ configure request
- **Identifier**: changes with every new request
- **Length**: overall length of the configure request message
- **Type**: 3 ~ DESEv2
- **Length’**: 10 (the length of this configuration option)
- **Initial Nonce**: an initialization vector for DES in CBC mode (8 octets)
Point-to-Point Protocol: Encryption Protocols (3)

- PPP DESE v2 message format:
  - Address: 0x11111111 (in case of HDLC-like framing)
  - Control: 0x00000011 (in case of HDLC-like framing)
  - Protocol ID: 0x0053 ~ DESE (standard) / 0x0055 ~ DESE (individual link)
  - Sequence Number: initially 0, this number is incremented by the encrypting entity with every packet sent
  - Ciphertext: the encrypted protocol and information fields of a PPP packet
    - messages are padded to a multiple of 8 octets prior to encryption
    - encryption is realized with DES in CBC mode
Point-to-Point Protocol: Encryption Protocols (4)

- PPP 3DES Encryption Protocol (3DESE):
  - PPP 3DESE [RFC2420] is very similar to the PPP DESE
  - PPP 3DESE is negotiated with a configure request message with the type field of the option set to 2 (~ 3DESE)
  - Encryption of PPP payload is like DESE, with the difference that 3DES is used with 3 different keys

- All of the PPP encryption protocols assume, that a session key for encryption / decryption of PPP packets has been agreed upon prior to the encryption phase:
  - This assumption is reasonable, as session key establishment is a task that should be fulfilled during the authentication phase
  - However, only the PPP-EAP-TLS authentication protocol supports session key establishment
Point to Point Tunneling Protocol (PPTP)

- PPP was originally designed to be run between “directly” connected entities, that is entities which share a layer-2 connection
  - Example: a PC and a dialup-router of an Internet service provider connected over the telephone network using modems
- The basic idea of PPTP is to extend the protocol’s reach over the entire Internet by defining transport of PPP PDUs in IP packets
  - Thus, the payload of PPTP PDUs are PPP packets (without layer-2 specific fields like HDLC flags, bit insertion, control characters, CRC error check values, etc.)
  - PPP packets are encapsulated in GRE packets (generic routing encapsulation) that themselves are encapsulated in IP packets:

<table>
<thead>
<tr>
<th>Media Header (e.g. Ethernet MAC header)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Header</td>
</tr>
<tr>
<td>GRE V.2 Header</td>
</tr>
<tr>
<td>PPP Packet</td>
</tr>
</tbody>
</table>
PPTP: Voluntary vs. Compulsory Tunneling

- PPTP realizes a “tunnel” over the Internet that carries PPP packets.
- Such a tunnel can be realized between different entities:
  - A client PC and a PPTP Remote Access Server (RAS):
    - This is also referred to as *voluntary tunneling*, as the client PC is actively participating in the PPTP processing.
    - This variant allows to support secure communication between a client PC and a specific subnetwork using any access and intermediate network(s).
  - An ISP’s Point of Presence (POP) and a PPTP Remote Access Server:
    - This is also referred to as *compulsory tunneling*, as the client PC is not involved in the decision whether PPTP will be used or not.
    - This allows to realize security on the subnetwork level but does not realize true end-to-end security between the client PC and the RAS.
    - In compulsory tunneling the ISP POP acts as a proxy client to the RAS.
PPTP: Compulsory Tunneling Protocol Layers

Client → ISP POP → PPTP-Tunnel → PPTP RAS → Application Server

IP / IPX / NetBEUI packet flow

PPP → PPTP

---

<table>
<thead>
<tr>
<th>Layer 1</th>
<th>Layer 2</th>
<th>Layer 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP / IPX / NetBEUI</td>
<td>PPP</td>
<td>Physical Layer</td>
</tr>
<tr>
<td>PPP Framing (e.g. HDLC)</td>
<td>GRE Version 2</td>
<td>Layer 2</td>
</tr>
<tr>
<td>Physical Layer</td>
<td>Layer 2 (e.g. 802.x)</td>
<td>Physical Layer</td>
</tr>
</tbody>
</table>

PPTP: Voluntary Tunneling Protocol Layers

Internet

Client ISP POP PPTP RAS Application Server

IP / IPX / NetBEUI packet flow

PPTP

PPP

IP / IPX / NetBEUI

PPP

GRE Version 2

IP

PPP Framing (HDLC)

Physical Layer

Layer 2 (e.g. 802.x)

Physical Layer

Physical Layer
PPTP: Voluntary Tunneling Packet Construction at Client

![Diagram showing PPTP packet construction](image)

PPTP / PPP Proprietary Extensions & Some “History”

- PPTP has been largely deployed as a consequence of Microsoft’s support for it:
  - It has been developed with Microsoft’s active involvement and is documented in [RFC2637]
  - Microsoft implemented it as a part of its Remote Access Service (RAS)
- Microsoft further specified “proprietary” extensions for PPP:
  - Microsoft PPP CHAP Extensions [RFC2433]
  - Microsoft Point to Point Encryption Protocol [RFC3078]
- However, a series of vulnerabilities have been discovered in PPTP version 1 and also in an improved version 2 [SM98a, SMW99a]:
  - A general consensus to adopt PPTP as a standard protocol could not be reached in the IETF working groups
  - Furthermore, a similar protocol (Layer 2 Forwarding, L2F) had been proposed by Cisco as a competing approach
  - As a consequence, a compromise was found to merge the advantages of both proposals into one single protocol Layer 2 Tunneling Protocol (L2TP)
Comparison of PPTP and L2TP

- Both protocols:
  - use PPP to provide an initial envelope for user packets
  - extend the PPP model by allowing the layer-2 and the PPP endpoints to reside on different devices
  - support voluntary and compulsory tunneling

- Underlying network:
  - PPTP requires an IP network to transport its PDUs
  - L2TP supports different technologies: IP (using UDP), Frame Relay permanent virtual circuits (PVCs), X.25 virtual circuits (VCs), or ATM VCs

- PPTP can only support a single tunnel between end points, L2TP allows for the use of multiple tunnels between end points
  - E.g. L2TP allows to create different tunnels for different qualities of service

- Both protocols provide for header compression:
  - With header compression L2TP operates with 4 bytes of overhead, as compared to 6 bytes for PPTP

- L2TP provides for tunnel authentication, while PPTP does not
Virtual Private Networks

- Various definitions of the term *virtual private network (VPN)*:
  - A private network constructed within a public network infrastructure, such as the global Internet
  - A communications environment in which access is controlled to permit peer connections only within a defined community of interest, and is constructed through some form of partitioning of a common underlying communications medium, where this underlying communications medium provides services to the network on a non-exclusive basis
  - A restricted-use, logical computer network that is constructed from the system resources of a relatively public, physical network (such as the Internet), often by using encryption, and often by tunneling links of the virtual network across the real network [RFC2828]
  - Remark: the later two definitions explicitly incorporate security properties (controlled access, encryption) while the first one does not

“Sure, it’s a lot cheaper than using your own frame relay connections, but it works about as well as sticking cotton in your ears in Times Square and pretending nobody else is around.” (Wired Magazine Feb. 1998)
Techniques for building Virtual Private Networks

- Make use of dedicated links (*cut-through mechanisms*):
  - ATM or Frame Relay virtual connections
  - Multi-Protocol Over ATM (MPOA)
  - Multi-Protocol Label Switching (MPLS)
  - Security services for link layer VPNs might efficiently be realized in the link layer protocol; one example is the ATM Security Specification [ATM99a]

- *Controlled route leaking / route filtering*:
  - Basic idea: control route propagation to the point that only certain networks receive routes for other networks
  - This intends to realize "security by obscurity"

- *Tunneling*:
  - Generic routing encapsulation (GRE)
  - PPP / PPTP / L2TP
  - IPSec Security Architecture for the Internet Protocol (see next chapter)
Additional References (1)


Additional References (2)


