Network Working Group
INTERNET-DRAFT

Solange Ghernaouti-Hélie
Mohamed Ali Sfaxi
University of Lausanne

Expires: April, 29 2006

October 2005

Quantum Key Destribution within Point to Point Protocol (Q3P)
draft-ghernaouti-sfaxi-ppp-qkd-00.txt

Abstract

The aim of this paper is to analyse the use of quantum cryptography within PPP. We propose a solution that integrates quantum key distribution into PPP.

Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [9].

1. Introduction

The point to point protocol (PPP) [RFC1661] is a data-layer protocol ensuring a reliable data exchange over a point to point link. When the connection is established and configured, the PPP allows the data transfer of many protocols (IP, IPX, AppleTalk). That's why; PPP is widely used in Internet environment.

The unique security of PPP as specified in the RFC 1661 is limited to the authentication phase. The two nodes use an authentication protocol such as Password Authentication Protocol (PAP) [RFC1334] or Challenge Handshake Authentication Protocol (CHAP)[RFC1994]. In 1996, Meyer published an additional security protocol for PPP called ECP (Encryption Control Protocol) [RFC1968]. This protocol allows the use of the encryption in PPP frame. The ECP gives the possibility to select the encryption algorithm and its parameters. This ensures the confidentiality and the integrity of the PPP frame. The weakness of this use resides in the way of generating and exchanging the encryption key. In fact, for all the encryption algorithms the secret key is assumed to be already shared between the communicating parties. So to enhance security, we propose the use of quantum cryptography to generate and to share the secret key between the two nodes.

Quantum cryptography is the only method allowing the distribution of a secret key between two distant parties without transmitting any secret over unsecure channel [1, 4]. the emitter and the receiver will be able to share an encryption key for enciphering confidential data. The secrecy of this shared key is unconditional [8] by the fact that the secret is generated and exchanged based on physic laws (instead of mathematical functions). That s why we propose to integrate the quantum key distribution (QKD) process to share secret key between two nodes.

2. Encryption Control Protocol (ECP) for Quantum Key Distribution (QKD)

The Encryption Control Protocol (ECP) defines the negotiation of the encryption over PPP links. After using LCP to establish and configure the data link, the encryption options and mechanisms could be negotiated. The ECP packets exchange mechanism is nearly the same as the LCP mechanism. The ECP packets are encapsulating into PPP frame (a packet per frame). The type is 0x8053 to indicate the Encryption Control Protocol. Two additional messages are added to the code field: the Reset-Request and Reset-Ack message. These two messages are used to restart the encryption

negotiation. An encrypted packet is encapsulated in the PPP information field where the PPP protocol field indicates type 0x0053 (encrypted datagram). The ECP packet is presented in figure 1

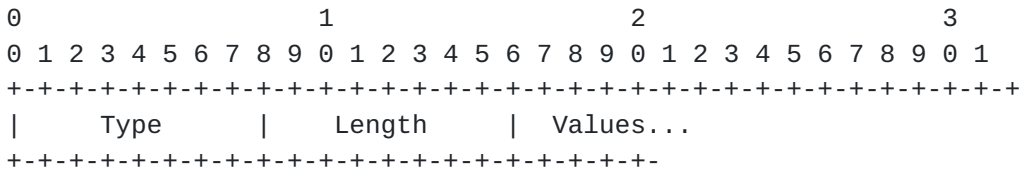


Figure 1 - The Encryption Type Configuration Option format

ECP packet, the type represents the encryption protocol option to be negotiated (for instance type 1 is DES encryption). The number of octets in the packet is contained in the length field. The values field gives additional data or option needed for the encryption protocol. Up to now, there are only 4 encryption algorithms (type 0 = OUI, type 1 = DES, type 2 = 3DES, type 3 = DES modified) that could be used [5].

3. Integrating QKD in PPP: QKD-PPP (Q3P)

In order to exchange the encryption key, a key exchange protocol is necessary. In this section, we present how to integrate QKD in PPP

3.1 ECP-QKD format

To establish and configure the quantum key distribution between the two nodes, it is necessary to exchange some data between them. We propose a specific ECP packet format to carry QKD parameters (Figure 2):

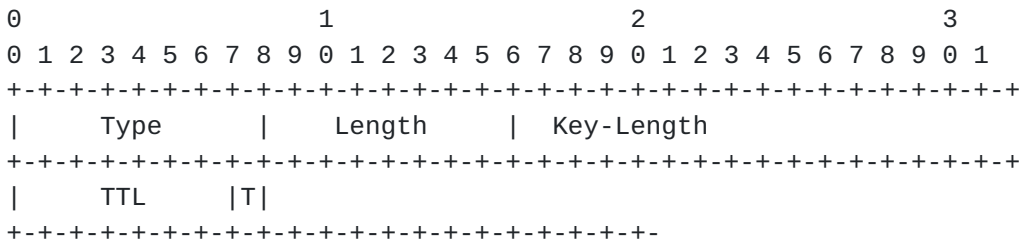


Figure 2 - ECP packet carrying a QKD protocol

Type field:
As in the ECP standard packet the type field gives information about the option of encryption protocol negotiated. For this case, we will use an unassigned number for the QKD protocol. The selected QKD protocol is BB84 and the request to obtain an assigned number for this protocol is on going in IANA organisation [5].

Length field:
The length is number of octets in the packet and it is more than 5 octets (1 octet for the type, 1 octet for the packet length, 2 octets for the key length and one octet for the TTL and the T field).

Key-length field:

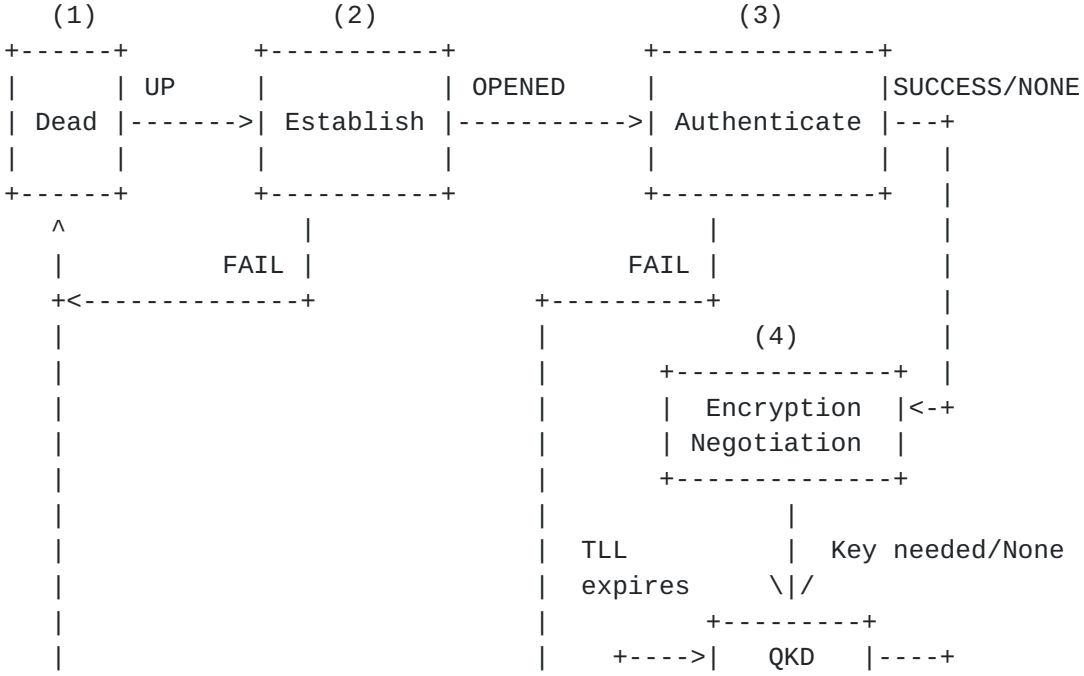
This field indicates the length of the encryption key. It is ended on 16 bits and represents the size of the key in octet. The key size is comprised between 1 to 65535 octets. The size can be viewed as huge but we consider the possibility to use the One Time Pad function as the encryption algorithm. In this case, the key size must be equal to the PPP-data size [11].

TTL field:
This field can represent either the number of messages or the amount of time (in second) during which a key could be used in the encryption mechanism. When the max number of messages is reached or the deadline expires, the QKD starts.

T field:
The T field specifies if the TTL field concerns the number of messages or the amount of time. If the value is 1 , the TTL field corresponds to the amount of time in second. If it is 0 , the TTL is the number of messages per key.

3.2 The Q3P operating mode

We adapt PPP connection steps [RFC1661] to integrate QKD process as shown Figure 3. The three first steps of Q3P are identical with PPP (phase 1 to 3). After authenticating the two nodes, the negotiation of the encryption parameters starts. In this phase, the encryption algorithm with its parameters is negotiated. If the two nodes do not need to use encryption, then the network phase starts. Else, if an encryption key is required, a QKD phase begins. For Encryption negotiation (4) the nodes negotiate the key length and the TTL by sending an adequate ECP packet. After that (in 5), a quantum cryptography exchange starts. At the end of the quantum key distribution phase, both nodes share a secret key, the encryption algorithm and the TTL of the key. This key is used in the network phase (6) while sending data. The data is enciphered thanks to the encryption key and the algorithm. When the TTL is expired, a new QKD phase starts. The end of the communication is the same as the PPP.



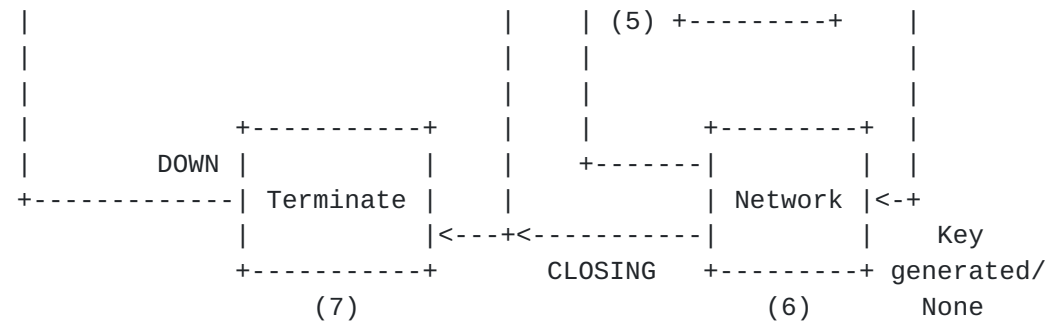


Figure 3 - Proposed Q3P steps and operating mode

The Figure 4 gives more details about Q3P operating mode. The modification are little so that the adaptation of the PPP operating mode is easy to realise.

1- Dead state (Initial state):
  a. When detecting an Up event then go the Establish phase
2- Establish phase:
  a. Configuration packets are exchanged (LCP)
  b. When finishing configuring the link connection go to the Authentication phase
3- Authentication phase:
  a. If required, the peer has to authenticate himself.
  b. If the authentication succeed or it is not required then go to Encryption negotiation phase else go to terminate phase
4- Encryption Negotiation phase:
  a. If required, the two nodes negotiate the encryption protocol parameters and the quantum key exchange parameters (such as TTL, Key length). If not required, go the Network phase
  b. After the end of the negotiation, go to QKD phase
5- QKD phase:
  a. The source and the detector share a secret key exchanged using quantum cryptography
  b. When the secret key is ready go to Network phase
6- Network phase:
  a. The two node exchange data
  b. When the encryption TTL expires go to QKD phase
  c. If the communication is finished, go to terminate phase (a close event is generated)
7- Terminate phase:
  a. Terminate messages are exchange, when finish go to Dead state

Figure 4 : The Q3P algorithm

4. Conclusion

For some needs, it is important to have the option to secure efficiently the data transmission between two adjacent nodes. Using quantum cryptography in conjunction with PPP offer a higher level of security. Our study points out the adaptation of the PPP protocol to integrate quantum key exchange (Q3P). The modifications to PPP are identified (packet format and operating mode).
Applying quantum key exchange and one-time-pad function at OSI layer 2 is not only possible but will upgrade considerably, with a low cost and less effort (modification, performances,), the security level of a transmission between two adjacent nodes.

5. Security considerations

Our proposition do not damage PPP security mechanism but enhance if by the use of quantum key echange.
The unconditional security of quantum key distribution has been already proven.

6. Authors Address

Solange Ghernaouti-Helie
HEC,
University of Lausanne
1015 Lausanne, Switzerland.
EMail: sgh@unil.ch

Mohamed Ali Sfaxi
HEC,
University of Lausanne
1015 Lausanne, Switzerland.
EMail: mohamedali.sfaxi@unil.ch

7 . References

[1] Bennet, C; Brassard, G (1984). IEEE International Conference on Computers, Systems, and Signal Processing. IEEE Press, LOS ALAMITOS

[2] Elliott, C (2002). Building the quantum network . New Journal of Physics 4 (46.1-46.12)

[3] Elliott, C; Pearson, D; Troxel, G (2003). Quantum Cryptography in Practice .

[4] Gisin, N; Ribordy, G; Tittel, W; Zbinden, H. (2002). Quantum Cryptography . Reviews of Modern Physics 74 (2002).

[5] Ghernaouti H´elie, S; Sfaxi, M.A; Ribordy, G; Gay, O (2005). Using Quantum Key Distribution within IPSEC to secure MAN communications . MAN 2005 conference.

[6] Guenther, C (2003) The Relevance of Quantum Cryptography in Modern Cryptographic Systems . GSEC Partical Requirements (v1.4b).
http://www.giac.org/practical/GSEC/Christoph_Guenther_GSEC.pdf

[7] Internet Assigned Numbers Authority - IANA (2005).
http://www.iana.org/numbers.html

[8] Paterson, K.G; Piper, f; Schack, R (2004). Why Quantum Cryptography? . http://eprint.iacr.org/2004/156.pdf

[9] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, Internet Engineering Task Force, March 1997.

[10]Schneier, B (1996). Applied Cryptography Second Edition. New York: John Wiley & Sons, 1996

[11]Shannon, C.E (1949). Communication theory of secrecy systems . Bell System Technical Journal 28-4.

Intellectual Property Statement

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.