Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 18, 2011

Y. Cui
J. Dong
Tsinghua University
Dayong. Guo
Huawei Technologies Co., Ltd
October 15, 2010

pcp subscriber identification
draft-cui-pcp-subscriber-identification-00

Abstract

This document analyzes on PCP security problems related with subscriber identification, such as denial-of-service(DoS), unwanted deleting of mappings, man-in-the-middle(MITM), and stale mapping problem. Then several solutions are proposed.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 18, 2011.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1. Introduction

PCP is primarily designed to be implemented in the context of large scale NAT deployments. It offers the ability to configure a port forwarding capability in Service Provider NATs. In a Service Provider case, subscriber identification and security are two of the important features. It's the basic of providing port service and accounting.

In Section 8.3 Subscriber Identification of current PCP protocol[I-D.draft-wing-softwire-port-control-protocol], PCP server uses IP address or prefix to identify PCP subscribers. However, PCP is a lightweight protocol and no connection is required to be maintained between the Client and the Server. It's very easy to create a fake IP address in many cases, so PCP server could not differentiate between legitimate requests and fake requests. Due to these reasons, ISPs need more reliable technology to enhance the security.

Generally in ISP networks, Broadband Network Gateway(BNG), aka Broadband Remote Access Server, provides the access authentication for subscribers. The BNG can identify by means of subscribers information besides IP address, for example MAC address, Circuit ID of access device which subscribers are attached to [RFC3046], etc. If PCP server is embedded into BNG, it can identify a PCP client with the information provided by BNG. In this case, PCP operations have high security.

However, PCP server is usually coupled with Service Provider NAT rather than BNG. When PCP server is separated from BNG, it can only identify PCP client by IP address, which may cause significant security problems.

This document mainly focuses on the security problems in the separated scenario and methods on how to solve these problems.

2. Security problem analysis of PCP separated scenario

PCP is a simple protocol based on UDP. It achieves its purpose by one simply request/response procedure. In separated scenario, these steps are vulnerable to denial-of-service (DoS), unwanted deleting of mappings, man-in-the-middle(MITM), and have stale mapping problem.

2.1. DoS attacking with address spoofing

Section 11.4 of PCP recommends IPv6 source address validation to protect against creating unwanted mappings. However, an adversary can flood the PCP requests with bogus source address, which satisfies the validation rules, to cause DoS attacks exhausting mapping resources. PCP server will allocate mappings for these illegal requests. The limited mapping resources will soon be exhausted, causing legitimate subscribers not having available resources.

2.2. Unwanted Deleting of Mappings

In PCP, requests with internal IP address and lifetime set to zero are used to delete all mappings of a subscriber. An adversary can flood the PCP requests with bogus source address deleting legitimate mappings. By trying a large number of source addresses, an adversary may successfully delete some legitimate mappings. This kind of attack will disrupt the normal PCP uses.

2.3. MITM attack

An adversary may try to eavesdrop and collect PCP requests. The normal request message contains some internal port numbers the PCP client wants to request. Adversary may increase a large number of fake internal ports and replay these requests. Then PCP server has to allocate some additional mappings that are unnecessary. If a large number of PCP requests are modified, the mapping resources would be exhausted. On the other way, by setting the lifetime and internal address to zero, an adversary may successfully delete some mappings to disrupt normal PCP uses.

2.4. Stale Mappings

Section 11.6 of [I-D.wing-softwire-port-control-protocol] has described this problem.

3. Possible solutions

This section will introduce several possible solutions to authenticate legitimate clients. According to different operating environment, ISPs could choose different method.

3.1. Authentication model for PCP

User name and password of a subscriber can be used to enhance PCP security. As shown in figure 1, PCP client sends request message with an extended Informational Element(IE) including user name and password to the PCP server. Then PCP server, as an AAA client, authenticates with AAA server via Diameter[RFC3588]/Radius protocol[RFC2865]. Only when the authentication succeeds can the PCP server start to allocate mappings to PCP client.

```
                        +---------+
                        |         |
                        |   AAA   |
                        |  server |
                        +---------+
                             |
                             |
                             |
                             |
     +---------+          +---------+            +----------+
     |   PCP   |          |   PCP   |            |          |
     |  client |----------|  server |-------------| Internet |
     |         |          |         |            |          |
     +---------+          +---------+            +----------+
```

Figure 1: Authentication model

With the adoption of the user name and password identification procedure, the DoS attack, unwanted mapping deleting and stale mapping problem can be well defended against. This procedure doesn't change the original PCP procedure for there are no new steps. However, it adds AAA procedure.

3.2. Random number

With this method, when PCP server receives a PCP request from a subscriber for the first time, it will reply an Error Response with a random number without allocating mappings to the PCP client. The random number can be contained in an IE. When a PCP client receives this response with random number, it will resend another PCP request with the same random number IE. The IE should be stored for later PCP communication.

With the random number method, when DoS attack with faked source address arrives, PCP server will not allocate mappings immediately. On the contrary, it replies a packet to the faked source address to ask the PCP client for another request with the random number, which the attackers will never receive. Furthermore, random number is valuable against unwanted deleting of mappings.

However, it cannot defend MITM attacks. This method increases steps of PCP communication procedure at the first time.

3.3. Safe tunnel negotiation

This method suggests a safe tunnel like TLS or IPsec to be established between PCP client and server before the starting of PCP communication. Based on the established safe tunnel, the PCP communication would be safe. All the problems stated in section 2 could be solved. Note that the negotiation procedure could be separated from PCP communication.

As we known that PCP is designed as a lightweight protocol. However, safe tunnel negotiation would makes the whole PCP procedure complicate. Especially, PCP server needs to process a large number of encrypted/decrypted information to establish safe tunnel. The costs for safe tunnel establishing may be more than that of PCP procedure itself.

3.4. Digit signature

The digit signature method suggests that PCP request and response messages should have an extended IE including digitally signed random number. The random number is firstly generated by PCP server. Every time when PCP server needs to send a response, it should generate a new random number and signs this random number. Figure 2 is a simple procedure of the digit signature method.

```
+---------+                                                +---------+
|   PCP   |                                                |   PCP   |
|  client |                                                |  server |
|         |                                                |         |
+---------+                                                +---------+
   |     PCP request with digitally signed random number        |
   | -------------------------------------------------------->  |
   |                                                            |
   |                                                            |
   |    PCP response with digitally signed random number        |
   | <--------------------------------------------------------  |
```

Figure 2: Digit signature method

This method is considered to be more secure than random number method and not as complicated as safe tunnel negotiation method.

4. Security Considerations

To be defined.

5. IANA Considerations

No IANA requirement.

6. Acknowledgments

7. References

7.1. Normative References

[I-D.wing-softwire-port-control-protocol]
Wing, D., Penno, R., and M. Boucadair, "Pinhole Control Protocol (PCP)", draft-wing-softwire-port-control-protocol-02 (work in progress), July 2010.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

7.2. Informative References

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3046] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, January 2001.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

Authors' Addresses

Yong Cui
Tsinghua University
Department of Computer Science, Tsinghua University
Beijing 100084
P.R.China

Phone: +86-10-6260-3059
Email: yong@csnet1.cs.tsinghua.edu.cn

Jiang Dong
Tsinghua University
Department of Computer Science, Tsinghua University
Beijing 100084
P.R.China

Phone: +86-10-6278-5822
Email: dongjiang@csnet1.cs.tsinghua.edu.cn

Dayong Guo
Huawei Technologies Co., Ltd
Huawei Building, No.3 Xinxi Rd., Shang-Di Information Industry Base, Hai-Dian District
Beijing 100085
P.R.China

Email: guoseu@huawei.com