ALTO
Internet-Draft

Intended status: Standards Track

Expires: August 27, 2010

Shuyi. Chen
Feng. Gao
ZTE Corporation
Xiaofeng. Qiu
Miao. Xiong
MINE Lab, BUPT

March 1, 2010

Overview for ALTO security issues
draft-chen-alto-security-overview-00

Status of this Memo

This Internet-Draft will expire on April 19, 2010.

Copyright Notice

Abstract

This document provides an overview of the security mechanisms that are probably fit for ALTO. Specifically it discusses those mechanisms for authentication, encryption and attack-preventing. The goal of this draft is to list and analyze the existing security mechanisms, and to explore suitable solutions to guarantee the security of ALTO protocol. This draft is a very early draft to outline the possible security mechanisms and leaves considerable contents and details to be added later.

Table of Contents

1. Introduction

Helping peer-to-peer (P2P) application to select better peers from a set of candidates is currently one of most popular research areas. The goal of Application-Layer Traffic Optimization (ALTO) [I-D.ietf-alto-problem-statement] is to provide guidance to p2p applications, which is based on parameters that affect performance and efficiency of the data transmission between the hosts, e.g., the topological distance. However, ALTO may be insecure when the clients are trustless or unauthorized. In this case, clients can steal ISP's ALTO information by snoop or deceit that would do harm to ALTO structure.

This draft gives the security issues between ALTO server and client which MAY be unauthorized. Part of these issues had been discussed in the mailing list, but this draft will give a summary of ALTO security issues with all kinds of situations. Since ISP privacy and P2P privacy issues had been discussed a lot in [I-D.wang-alto-privacy-load-analysis], this draft will focus mainly on security issues among unauthorized parties. Additionally the common authentication/encryption and attack- preventing mechanisms which are suitable for ALTO protocol are given below.

2. Terminology and Concepts

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 [RFC2119].

This document also reuses the concepts defined in [I-D.ietf-alto-problem-statement] and [I-D.ietf-alto-reqs].

3. ALTO security requirements

ALTO protocol has some minimum-to-implement security requirements. This set of security requirements has been listed in Section 3.3 in [I-D.ietf-alto-reqs].

General ALTO security requirements include four parts:
(1) Preventing an ISP's internal topology from being leaked
(2) Preventing an ISP from learning about P2P application behavior (e.g., the information about peers with which it is connecting)
(3) Preventing unauthorized access to ISP's ALTO information. There are a couple of cases here:
  (a) An ALTO Server sends the information directly to an unauthorized ALTO Client
  (b) An unauthorized party snoops on the data transmission from the ALTO Server to an authorized ALTO Client.
  (c) An authorized ALTO Client knowingly sends the information to an unauthorized party
(4) Preventing an ALTO Server from being attacked by malicious behavior due to the insecure design of ALTO protocol (e.g., DoS)

Here is the figure describing this situation:

```
                     +--------------------+
                     |    Attacker        |
                    /|                    |\
                   / +--------------------+ \
                 (4)                        (4)
                 /                            \
   +-------------+                           +------------------------+
   | ALTO server | -------(1)----[snoop]-- > | Authorized ALTO client |
   |    ISP      | <------(2)----[snoop]---- |    P2P application     |
   +-------------+                 |         +------------------------+
       \                           |                   /
        \                        (3b)                 /
        (3a)                       |               (3c)
           \                       |               /
            \--------- > +--------------+ <----------/
                         | Unauthorized |
                         |    Party     |
                         +--------------+
```

Figure 1. ALTO security requirements between ALTO entities

According to classification of ALTO security issues, (1)(2) have nothing to do with authentication/encryption because they only concern about the ALTO servers and authorized ALTO clients. Transmission over them only refers to the content but not the roles. While in part 3, (3a) and (3b) are closely related to authentication/encryption, but (3c) is not. There are not many methods for authorized ALTO client to prevent ISP's ALTO information from being leaked to unauthorized parties. Since when ALTO client requests the desired information, ALTO server will surely send out desired information to the requester no matter whether it is authorized or not. (4) is an independent security part, which refers to mechanisms for ALTO Server against attacks like DoS. There are solutions mentioned in other draft for (1)(2) in most cases, and some solutions for (3)(4) will be given below.

4. ALTO security mechanisms

Client in ALTO may be unauthorized that means it can cheat the server to threaten the ALTO security. Based on the four parts above, ALTO security mechanisms at least contain authentication, encryption and attack-preventing.

4.1. Authentication mechanism

4.1.1. No Authentication

The simplest case is that all clients in ALTO are trustworthy or a kind of filtering is done before clients join the network. In this case, authentication is needless.

4.1.2. HTTP Digest Access Authentication

HTTP Digest Access Authentication is one of the agreed methods that a web server can use to negotiate credentials with a web user (using the HTTP protocol). Digest authentication is intended to supersede unencrypted use of the Basic access authentication, allowing user identity to be established securely without having to send a password in plaintext over the network.

HTTP provides a simple challenge-response authentication mechanism that MAY be used by a server to challenge a client request and by a client to provide authentication information. That is quite suitable for ALTO framework since ALTO is also the server/client framework. When the ALTO server receives the requested message, it will challenge the client who initiates the request and the client in the same time will give the response providing its authentication information.

The Digest scheme challenges using a nonce value. A valid response contains a checksum (by default, the MD5 checksum) of the username, the password, the given nonce value, the HTTP method, and the requested URI.

HTTP Digest Access Authentication is simple and secure in web-level applications providing a more complex authentication than Basic authentication, and it introduces the server/client nonce which will prevent replay and chosen plaintext attacks. However it has many known limitations. Digest access authentication is intended as a security trade-off, therefore it is no secure than public key or Kerberos authentication. But Digest access authentication will make ALTO protocol lightweight so that security will not bring ALTO protocol too much overhead.

4.2. Encryption mechanism

4.2.1. SSLv3/TLS

SSL(Secure Socket Layer)and TLS(Transport Layer Security)are widely used cryptographic protocols that provide security for several applications in the Internet like web browsing, VoIP, e-mail. SSLv3 is the third version of SSL and developed by Netscape Corporation. TLS is an IETF standards track protocol, last updated in RFC 5246.

The TLS protocol allows client/server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. TLS provides endpoint authentication and communications confidentiality over the Internet using cryptography. Typically, the key information and certificates necessary for TLS are handled in the form of X.509 certificates, which define required fields and data formats.

SSL operates in modular fashion. It is extensible, with support for forward and backward compatibility and negotiation between peers.

SSL/TLS can provide:
(1) Authentication between server and client. That will ensure that the information is sent to the correct client or server.
(2) Data encryption. Before the secure connection is established, both parties use the asymmetric key cryptography. After the establishment, symmetric key cryptography will be used. That will keep ISP's information not leaked to unauthorized parties.
(3) Ensure data integrity. Using hash function makes data integrity.

SSL/TLS is a standard method to protect SIP application signaling. SSL/TLS can be used to provide authentication and encryption of the SIP signaling associated with VoIP and other SIP-based applications. Be similar to SIP, SSL/TLS can also be used to provide authentication and encryption of ISP's ALTO information that is communicated between server and client.

4.3. Attack-preventing mechanism

Since ALTO server may be the target of attack, ALTO should provide security mechanism to protect ALTO server from being attacked by malicious behavior (e.g., DoS). Due to the insecure design of ALTO protocol, there are several risks for attacker to harm ALTO. When ALTO client/server communicates, they establish a TCP connection. In response to query messages, an ALTO client/server constructs and sends messages containing TCP messages. And it makes DoS attacks possible if the attackers produce thousands of TCP request with fake IP addresses that their ACKs will never be received by the server. This makes the server wastes much time and CPU to wait for non-existent ACK. It harms great to ALTO system.

An useful mechanism for DoS attack includes SYN cookie and restraining the connection number in definite time and from definite source. Another widely used method is firewall.

5. Security Considerations

Most of the security issues have been discussed above.

6. IANA Considerations

There is no IANA action required by this draft.

7. References

7.1. Normative References

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

7.2. Informative References

[RFC5693]
Seedorf, J. and E. Burger, "Application-Layer Traffic Optimization (ALTO) Problem Statement", draft-ietf-alto-problem-statement , October 2009.

[RFC5246]
Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC2617]
Franks, J. and P. Hallam-Baker, "HTTP Authentication:Basic and Digest Access Authentication", RFC2617,June 1999.

[I-D.ietf-alto-reqs]
Kiesel, S., Popkin, L., Previdi, S., Woundy, R., and Y. Yang, "Application-Layer Traffic Optimization (ALTO) Requirements", draft-ietf-alto-reqs-02 (work in progress), October 2009.

[I-D.ietf-alto-protocol]
Alimi, R., Penno, R., and Y. Yang, "ALTO Protocol", draft-ietf-alto-protocol-01 (work in progress), December 2009.

[I-D.wang-alto-privacy-load-analysis]
Wang, Y., Song, H., and M. Chen, "Analysis for ALTO privacy and load issues", draft-wang-alto-privacy-load-analysis-00 (work in progress) October 2009.

Authors' Addresses

Shuyi Chen

ZTE Corpoporation
17/F, ZTE Plaza, No.19, East HuaYuan Road,
Haidian District, Beijing,
P.R.China, 100191
Phone:+86-10-82963667
Email: chen.shuyi@zte.com.cn

Feng Gao

ZTE Corpoporation
17/F, ZTE Plaza, No.19, East HuaYuan Road,
Haidian District, Beijing,
P.R.China, 100191
Phone:+86-10-82963777
Email: gao.feng1@zte.com.cn

Xiaofeng Qiu

Mobile lIfe and New mEdia Lab,
Beijing University of Posts and Telecommunication,
P.O. Box 92, No.10, Xitucheng Road,
Haidian District, BeiJing,
P.R.China, 100876
Email: qiuxiaofeng@gmail.com

Miao Xiong

Mobile lIfe and New mEdia Lab,
Beijing University of Posts and Telecommunication,
P.O. Box 92, No.10, Xitucheng Road,
Haidian District, BeiJing,
P.R.China, 100876
Email: xiongbearie@gmail.com