ALTO
Internet-Draft
Intended status: Standards Track
Expires: February 8, 2010

M. Stiemerling
NEC Europe Ltd.

August 7, 2009

ALTO Information Redistribution Considered Harmful
draft-stiemerling-alto-info-redist-00

Abstract

The merged ALTO protocol proposal proposes several mechanisms to increase scalability of the protocol. One of the proposed mechanisms is the distribution of ALTO information directly between the peers without any involvement of the server. This memo discusses why the proposed mechanism is considered harmful and why the proposed security framework is deployable.

Table of Contents

1. Introduction

Scalabilty for the ALTO protocol is of major concern, as a single ALTO server potentially has to serve a large number of ALTO clients. The order of magnitude of how many clients will be served by a single ALTO server is not yet clear, but it can be expected that a single server must be able server a multiple of 10,000 clients simultaneously. The merged ALTO protocol proposal [I-D.penno-alto-protocol] proposes several mechanisms to increase scalability of the protocol. One of the proposed mechanisms is the distribution of ALTO information directly between the peers without any involvement of the server and any need to contact the server when having received the information.

The next section explores why the proposal is considered harmful.

Comments and discussions about this memo should be directed to the ALTO working group: alto@ietf.org.

2. Considered Harmful

Section 10.4 in [I-D.penno-alto-protocol] proposes this:

> It is possible for applications to redistribute ALTO information to improve scalability. Even with such a distribution scheme, ALTO Clients obtaining ALTO information must be able to validate the received ALTO information to ensure that it was actually generated by the correct ALTO Server. Further, to prevent the ALTO Server from being a target of attack, the verification scheme must not require ALTO Clients to contact the ALTO Server.

This paragraph calls for the ability to distribute ALTO information obtained via the ALTO protocol directly between the peers (called applications in the above text) without any ALTO server involvement. This approach looks promising as it allows to reach more potential clients with the ALTO information. However, there is no mean for the peers to verify whether the information provided is actually intended for their usage nor if the information is actually accurate at their current topological position in the Internet.

For instance, peer A located in ISP1 obtains ALTO information from a peer B. Peer B is located in ISP2 and provides the information is has obtained from its local ALTO server. Peer B and peer A do not have an easy way to determine whether they are located in the same ISP's network and thus they share ALTO information across ISP domains. Sharing of ALTO information across domains does not seem to be a natural goal of ALTO. This is considered harmful, as ALTO information that is usual intended to be used within a single ISP is re-distributed.

The draft proposes furthermore an assumed security solution that aims at preventing tampering with ALTO information:

> To fulfill these requirements, ALTO Information meant to be redistributable contains a digital signature which includes a hash of the ALTO information encrypted by the ALTO Server's private key. The corresponding public key should either be part of the ALTO information itself, or it could be included in the interface descriptor. The public key SHOULD include the hostname of the ALTO Server and it SHOULD be signed by a trusted authority.

First of all does this require public/private key pair, where the public key is known to each peer and a trusted third party is required. These requirements are possible to be fulfilled in certain deployments but are not in the general Internet deployment case, which in turn limits the applicability of this protocol. Second, the receiving peer needs to contact the ALTO server at least once to

obtain the public key part, or it does need to contact another server that provides the public key pair.

3. Security Considerations

This initial version of this memo does not yet have any security considerations, even though it tackles security issues.

4. Conclusion

Martin Stiemerling is partially supported by the NAPA-WINE project (http://www.napa-wine.org), a research project supported by the European Commission under its 7th Framework Program (contract no. 214412).

5. References

5.1. Normative References

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

5.2. Informative References

[I-D.penno-alto-protocol]
Penno, R. and Y. Yang, "ALTO Protocol", draft-penno-alto-protocol-03 (work in progress), July 2009.

Author's Address

Martin Stiemerling
NEC Laboratories Europe/University of Goettingen
Kurfuerstenanlage 36
Heidelberg 69115
Germany

Phone: +49 6221 4342 113
Fax: +49 6221 4342 155
Email: stiemerling@nw.neclab.eu
URI: http://www.net.informatik.uni-goettingen.de/people/martin_stiemerling