IPv6 Operations Working Group
Internet-Draft
Expires: August 28, 2008

S. Krishnan
Ericsson
J. Hoagland
Symantec
February 25, 2008

Teredo Security Updates
draft-krishnan-v6ops-teredo-update-02

Status of this Memo

Copyright Notice

Abstract

Additional security concerns with Teredo are documented, beyond what is in RFC 4380. This is based on an independent analysis of Teredo's security implications. The primary intent of this document is to describe the updates required to update the Teredo specification.

Comment [DT1]: Independent of what? The IETF?

Comment [DT2]: Awkward wording

Table of Contents

1. Introduction

An independent analysis of Teredo's security implications was conducted by Symantec[TEREDOSEC], based on the Teredo specification ([RFC4380]). This analysis uncovered some security concerns associated with Teredo which are not documented in the Teredo specification. This document discloses these additional concerns proposes the updates required to Teredo in order to address these concerns. This Internet Draft is also influenced to an extent by an examination of the Teredo implementation on Microsoft Windows Vista [WVNASA]. This draft recommends two changes to Teredo in order to make it more secure.

Comment [DT3]: This would be more appropriate in the Acknowledgements section than here.

2. Randomize flags

Teredo addresses are structured and some of the fields contained in them are fairly predictable. This can be used to better predict the address.

Teredo prefix: This field is 32 bits and has a single IANA assigned value

Server: This field is 32 bits and is set to the server in use. The server to use is usually statically configured on the client. This means that overall entropy of the server field will be low, i.e., that the server will not be hard to predict. Attackers could confine their guessing to the most popular server IP addresses.

Flags: The flags field is 16 bits in length, but RFC 4380 provides for only one of these bits (the cone bit) to vary.

Client port: This 16 bit field corresponds to the external port number assigned to the client's Teredo service port. Thus the value of this field depends on two factors (the chosen Teredo service port and the NAT port assignment behavior) and therefore it is harder to predict the entropy this field will have. If clients tend to use a predictable port number and NATs are often port-preserving ([RFC4787]), then the port number can be rather predictable.

Client IPv4 address: This 32 bit field corresponds to the external IPv4 address the NAT has assigned for the client port. In principle, this can be any address in the assigned part of the IPv4 unicast address space. However, if an attacker is looking for the address of a specific Teredo client, they will have to have the external IPv4 address pretty well narrowed down. Certain

IPv4 address ranges could also become well known for having a higher concentration of Teredo clients, making it easier to find an arbitrary Teredo client. These addresses could correspond to large organizations that allows Teredo such as a university or enterprise or to Internet Service Providers that only provide their customers with RFC 1918 addresses.

Optimizations in scanning can also reduce the number of addresses that need to be checked. For example, for addresses behind a cone NAT, it would likely be easy to probe if a specific port number is open on a IPv4 address, prior to trying to form a Teredo address for that address and port.

Most of this is elaborated on more in [TEREDOSEC].

3. Deprecate cone bit

The cone bit tells the attacker whether a bubble is needed to proceed a connection. It may also have some value in terms of profiling to the extent that it reveals the security posture of the network. If the cone bit is set, the attacker may decide it is fruitful to port scan the embedded external IPv4 address and others associated with the same organization, looking for open ports. Deprecating the cone bit would prevent the a priori revelation of the security posture of the NAT and would not reduce the functionality of the Teredo protocol. The qualification procedure described in section 5.2.1 of [RFC4380] will also be affected by this change.

Comment [DT4]: This is phrased as a proposal, not as a result.

Comment [DT5]: While I agree that the cone bit should be deprecated (and it isn't used in Vista), it's not true that nothing is reduced. The peer cannot distinguish between cone and restricted NATs. Teredo communication will still succeed, but at the expense of forcing peers to skip step 4 of the sending details in RFC4380, which results in extra indirect bubbles that would not otherwise be needed. Skipping step 4 is already allowed (by RFC4380 section 5.2.4) for reliability reasons, and hence this does not break interoperability, but the result of skipping the first phase of qualification is to force that behavior (which is less efficient, but potentially more reliable) to be taken by peers.

4. Proposed changes

The Flags field defined in section 4 of [RFC4380] is redefined as follows.

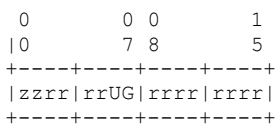

Figure 1: Flags format

- The bits "UG" should be set to the value "00", indicating a non-global unicast identifier.

- The bits marked "z" SHOULD be set to 0. This bit was earlier defined as the Cone bit to indicate if the client was behind a cone NAT.

- The bits marked with "r" SHOULD be chosen at random by the client.

Assuming there is no bias in those bit settings, then this adds 12 additional bits of entropy (4096 times as many addresses). This makes it harder for an attacker to guess Teredo addresses.

5. Backward Compatibility

The Microsoft web site [MSTO] indicates that Windows Vista already randomizes the bits as suggested in this document. Other implementations need to be updated to perform this. All client implementations need to be modified to always set the cone bit to 0, in order to be compliant with this document. But in either case, there are no functional interoperability issues and Teredo components updated as suggested in this specification are fully compatible with implementations that follow RFC 4380.

6. Acknowledgments

The authors would like to thank Remi Denis-Courmont, Dave Thaler, Fred Templin, Jordi Palet Martinez, James Woodyatt and Christian Huitema for reviewing earlier versions of the document and providing comments to make this document better.

7. Security Considerations

This document describes some updates to RFC4380 in order to improve the security of the base Teredo mechanism. Teredo is NOT RECOMMENDED as a solution for managed networks. Administrators of such networks may wish to filter all Teredo traffic at the boundaries of their networks.

8. IANA Considerations

There are no IANA considerations resulting from this document.

9. References

Comment [DT6]: This is wrong. RFC 4380 defines the second bit as MUST be zero. This relaxes it to a SHOULD, which is unnecessary and, in my view, harmful as it prevents any future extensibility.

Comment [DT7]: There's two z bits, only the first one was defined as the Cone bit.

Comment [DT8]: True, but you don't really need to cite that source. Can just delete the words before "Windows".

Comment [DT9]: Second 4 redefined the flags field so there is no cone bit, so this statement makes no sense in the new definition. Furthermore, since the cone bit is not in the flags, the behavior specified in RFC4380 that mentions the cone bit would need to be updated, which isn't done in this document. I think removing the cone bit from the flags definitions is the wrong approach.

9.1. Normative References

[RFC4380] Huitema, C., "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)", RFC 4380, February 2006.

[RFC4787] Audet, F. and C. Jennings, "Network Address Translation (NAT) Behavioral Requirements for Unicast UDP", BCP 127, RFC 4787, January 2007.

9.2. Informative References

[MSTO] Microsoft, "Teredo Overview", <http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/teredo.mspx>.

[TEREDOSEC] Hoagland, J., "The Teredo Protocol: Tunneling Past Network Security and Other Security Implications", November 2006, <http://www.symantec.com/avcenter/reference/Teredo_Security.pdf>.

[WVNASA] Hoagland, J., Conover, M., Newsham, T., and O. Whitehouse, "Windows Vista Network Surface Analysis", March 2007, <http://www.symantec.com/avcenter/reference/Vista_Network_Attack_Surface_RTM.pdf>.

Authors' Addresses

Suresh Krishnan
Ericsson
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Phone: +1 514 345 7900 x42871
Email: suresh.krishnan@ericsson.com

James Hoagland
Symantec Corporation
350 Ellis St.
Mountain View, CA 94043
US

Email: Jim_Hoagland@symantec.com
URI: http://symantec.com/

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).