Internet Engineering Task Force (IETF)
Request for Comments: 5991
Updates: 4380
Category: Standards Track
ISSN: 2070-1721

D. Thaler
Microsoft
S. Krishnan
Ericsson
J. Hoagland
Symantec

September 2010

Teredo Security Updates

Abstract

The Teredo protocol defines a set of flags that are embedded in every Teredo IPv6 address. This document specifies a set of security updates that modify the use of this flags field, but are backward compatible.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5991.

Table of Contents

1. Introduction

Teredo [RFC4380] defines a set of flags that are embedded in every Teredo IPv6 address. This document specifies a set of security updates that modify the use of this flags field, but are backwards compatible. This document updates RFC 4380.

The Flags field in a Teredo IPv6 address has 13 unused bits out of a total of 16 bits. To guard against address-scanning risks [RFC5157] from malicious users, this update randomizes 12 of the 13 unused bits when configuring the Teredo IPv6 address. Even if an attacker were able to determine the external (mapped) IPv4 address and port assigned by a NAT to the Teredo client, the attacker would still need to attack a range of 4,096 IPv6 addresses to determine the actual Teredo IPv6 address of the client.

The cone bit in a Teredo IPv6 address indicates whether a peer needs to send Teredo control messages before communicating with a Teredo IPv6 address. Unfortunately, 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, an 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 prevents the a priori revelation of the security posture of the NAT.

2. Terminology

This document uses the following terminology, for consistency with [RFC4380].

Cone NAT: A NAT that maps all requests from the same internal IP address and port to the same external IP address and port. Furthermore, any external host can send a packet to the internal host by sending a packet to the mapped external address and port.

Indirect Bubble: A Teredo control message that is sent to another Teredo client via the destination's Teredo server, as specified in [RFC4380], Section 5.2.4.

Local Address/Port: The IPv4 address and UDP port from which a Teredo client sends Teredo packets. The local port is referred to as the Teredo service port in [RFC4380]. The local address of a node may or may not be globally routable because the node can be located behind one or more NATs.

Mapped Address/Port: A global IPv4 address and a UDP port that results from the translation of a node's own local address/port by one or more NATs. The node learns these values through the Teredo protocol specified in [RFC4380]. The mapped address/port can be different for every peer with which a node tries to communicate.

Network Address Translation (NAT): The process of converting between IP addresses used within an intranet or other private network and Internet IP addresses.

Peer: A Teredo client with which another Teredo client needs to communicate.

Port-Preserving NAT: A NAT that translates a local address/port to a mapped address/port such that the mapped port has the same value as the local port, as long as that same mapped address/port has not already been used for a different local address/port.

Public Address: An external global address used by a NAT.

Restricted NAT: A NAT where all requests from the same internal IP address and port are mapped to the same external IP address and port. Unlike the cone NAT, an external host can send packets to

an internal host (by sending a packet to the external mapped address and port) only if the internal host has first sent a packet to the external host.

Teredo Client: A node that implements the client parts of [RFC4380], has access to the IPv4 Internet, and wants to gain access to the IPv6 Internet.

Teredo IPv6 Address: An IPv6 address that starts with the prefix 2001:0000:/32 and is formed as specified in Section 4 of [RFC4380].

Teredo Server: A node that has a globally routable address on the IPv4 Internet, and is used as a helper to provide IPv6 connectivity to Teredo clients.

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 [RFC2119].

3. Specification

3.1. Random Address Flags

Teredo addresses are structured, and some of the fields contained in them are fairly predictable. This makes the addresses themselves easier to predict and opens up a vulnerability.

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 generally 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 [RFC4380] provides for only one of these bits (the cone bit) to vary.

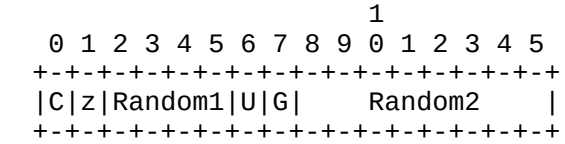
Client port: This 16-bit field corresponds to the external port number assigned to the client’s Teredo service port. Thus, the value of this field depends on two factors (the chosen Teredo

service port and the NAT port assignment behavior), and it therefore 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, 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 allow 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 an IPv4 address, prior to trying to form a Teredo address for that address and port.

Hence, the Flags field specified in [RFC4380], Section 4 is updated as follows:



C: This flag is specified in [RFC4380], and its use is modified in Section 3.2 below.

z: This flag is reserved. It MUST be set to zero when the address is constructed, as specified in [RFC4380].

Random1: MUST be set to a random value.

U: This flag is specified in [RFC4380].

G: This flag is specified in [RFC4380].

Random2: MUST be set to a random value.

3.2. Deprecation of Cone Bit

The qualification procedure is specified in [RFC4380], Section 5.2.1, and is modified as follows. Teredo clients SHOULD completely skip the first phase of the qualification procedure and implement only the second phase where it uses the Teredo link-local address with the cone bit set to zero. Consequently, a distinction between cone and restricted NATs can no longer be made. Teredo communication will still succeed, but at the expense of forcing peers to skip case 4 of the sending details specified in [RFC4380], Section 5.2.4. This will result in the same number of indirect bubbles being sent as if the other end were a peer behind a restricted NAT. Even though the peer behind the cone NAT does not need these indirect bubbles, it replies to these indirect bubbles just like it would to any other indirect bubbles. Skipping case 4 is already allowed for reliability reasons (as also specified in [RFC4380], Section 5.2.4), 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.

In addition, clients and relays SHOULD ignore the cone bit in the address of a Teredo peer and treat it as if it were always clear, as specified in [RFC4380], Section 5.2.4 (last paragraph).

Teredo servers MUST NOT ignore the cone bit for the following reasons.

- The cone bit in the IPv6 source address of a Router Solicitation (RS) from a client controls what IPv4 source address the server should use when sending a Router Advertisement (RA). If this behavior is not preserved, legacy clients will conclude that they are behind a cone NAT even when they are not (because the client WILL receive the RA where previously it would not, since a cone bit set to 1 requires the server to respond from another IP address). They will then set their cone bit and lose connectivity.

- When the Teredo server sends RAs (or bubbles if it’s also a relay), the cone bit in its own Teredo address is set, indicating that it doesn’t require bubbles to reach it.

4. Security Considerations

The basic threat model for Teredo is described in detail in [RFC4380], Section 7, but briefly, the goal is that a Teredo client should be as secure as if a host were directly attached to an untrusted Internet link. This document specifies updates to [RFC4380] that improve the security of the base Teredo mechanism regarding specific threats.

IPv6 address scanning [RFC5157] by off-path attackers: The Teredo IPv6 Address format defined in [RFC4380], Section 4 makes it relatively easy for a malicious user to conduct an address-scan to determine IPv6 addresses by guessing the external (mapped) IPv4 address and port assigned to the Teredo client. The random address bits guard against address-scanning risks by providing a range of 4,096 IPv6 addresses per external IPv4 address/port. As a result, even if a malicious user were able to determine the external (mapped) IPv4 address and port assigned to the Teredo client, the malicious user would still need to attack a range of 4,096 IPv6 addresses to determine the actual Teredo IPv6 address of the client. Appendix B compares the address prediction resistance of a Teredo address following this specification to that of an address formed using standard IPv6 stateless address autoconfiguration [RFC4862].

In order to prevent adversaries from easily guessing the values of the random bits and hence the address, the Random1 and Random2 bits in the Teredo Flags field MUST be constructed following the recommendations for random number generation as specified in [NIST-RANDOM] and [RFC4086].

Opening a hole in an enterprise firewall [TUNNEL-SEC]: Teredo is NOT RECOMMENDED as a solution for networks that wish to implement strict controls for what traffic passes to and from the Internet. Administrators of such networks may wish to filter all Teredo traffic at the boundaries of their networks.

5. Acknowledgments

The authors would like to thank Remi Denis-Courmont, Fred Templin, Jordi Palet Martinez, James Woodyatt, Christian Huitema, Tom Yu, Jari Arkko, David Black, Tim Polk, and Sean Turner for reviewing earlier versions of this document and providing comments to make this document better. The authors would also like to thank Alfred Hoenes for a careful review of this document.

6. References

6.1. Normative References

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

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

6.2. Informative References

[NIST-RANDOM] "NIST SP 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators", March 2007, <http://csrc.nist.gov/publications/nistpubs/800-90/SP800-90revised_March2007.pdf>.

[RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, June 2005.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[RFC5157] Chown, T., "IPv6 Implications for Network Scanning", RFC 5157, March 2008.

[TUNNEL-SEC] Hoagland, J., Krishnan, S., and D. Thaler, "Security Concerns With IP Tunneling", Work in Progress, March 2010.

Appendix A. Implementation Status

Deprecation of the cone bit as specified in this document is implemented in Windows Vista and Windows Server 2008.

The random flags specified in this document are implemented in Windows Vista SP1 and Windows Server 2008.

All Windows implementations automatically disable Teredo if they detect that they are on a managed network with a domain controller.

Appendix B. Resistance to Address Prediction

This section compares the address prediction resistance of a Teredo address as compared to an address formed using IPv6 stateless address autoconfiguration (SLAAC) [RFC4862].

Let’s assume that the attacker knows a Teredo client’s external IPv4 address and Ethernet card’s vendor. Since the attacker knows the client’s external IPv4 address, he does not have to search this space. The attacker does not know the external port (16 bits) and the value of the random bits (12 bits), and he has to search this space. This gives the attacker a total search space of 28 bits (16+12). This compares very favorably with the 24 bits of search space required to find an address configured using SLAAC (when the Ethernet card’s vendor is known) as described in Section 2.3 of [RFC5157]. Without the 12 random bits, the search space is limited to only 16 bits, and this is significantly worse than the 24 bits of search space provided by SLAAC.

As the knowledge of the attacker decreases, the number of bits of search space in both cases is likely to increase in a relatively similar fashion. The predictability of Teredo addresses will stay comparable to that of SLAAC addresses with the added 12 bits of search space, but will be significantly worse without the random bits.

Authors' Addresses

Dave Thaler
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
USA

Phone: +1 425 703 8835
EMail: dthaler@microsoft.com

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
USA

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