INTERNET DRAFT
draft-ohta-multi6-threats-00.txt
M. Ohta
Tokyo Institute of Technology
February 2004

Threats Relating to Transport Layer Protocols Handling Multiple Addresses

Status of this Memo

This document is an Internet-Draft and is subject to all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Abstract

This document lists security threats related to IPv6 multihoming solutions, transport layer protocols of which are expected to handle multiple addresses of a host and an identity of the host is recognized not necessarily by a single address.

The intent is to look at how IPv6 multihoming solutions might make the Internet less secure than the current Internet, without studying any proposed solution but instead looking at threats that are inherent in the problem itself.

1. Security Considerations

With the current Internet, most transport layer protocols identifies a host with a single address.

However, for scalable multihoming, transport layer protocols are expected to handle multiple addresses of a host and an identity of the host is recognized not necessarily by a single address.

Then, there are four new possibility of security threats.

Connection Hijacking with False Peer Address
hosts in multihomed sites may be supplied a false peer address

from an attacker, which redirect existing connection to a wrong location.

New DDoS Opportunity with False Source Information
hosts may be used for distributed DoS to damage the rest of the Internet

New DoS Opportunity on Identification
depending on a way to identify a host, the host may be subject to DoS

Privacy on Identification
depending on a way to identify a host, hosts may not be able to hide its privacy

The following subsections analyze the threats with or without MITM (Man in the Middle).

1.1. Connection Hijacking with False Peer Address

If a host has connected communicating with a peer, and if a transport layer protocol allows dynamic address set change during a connection, an attacker may be able to supply false information on source address of the peer to the host to hijack the connection.

On the current Internet, where connections are identified by a pair of addresses, which is fixed during connection, this kind of attack is not possible at the transport layer. However, similar attack is possible at upper layers. For example, an attacker may rewrite URLs in HTML text over HTTP over TCP to hijack a web browsing session. Or, an attacker may rewrite DNS reply of IP addresses during URL resolution or at the initiating phase of an application layer connection. As a protection against such attacks, transport and/or upper layer protocols use cookie or cookie like information, such as randomized port number, TCP sequence number, DNS message id and so on.

Without assuming MITM, existing transport and/or upper layer protocols using cookie or cookie like information can be naturally extended as a reasonable protection against connection hijacking by false source information.

Of course, cookie is powerless against MITM and once a forged source address, URL or DNS answer is supplied by MITM, the effect will be persistent even after the MITM goes away.

If transport layer protocols handling multiple addresses of a host does not have cookie or cookie like mechanism at least as strong as that of TCP and still allow dynamic address set change during connection, there will be a new security threat of connection hijacking.

1.2. New DDoS Opportunity with False Source Information

On the current Internet, an attacker can send a packet with forged source address expecting that a reply packet is sent to host of the source address, as DDoS attack to the host. There often is some

amplification possible. For example, DNS reply is often a lot longer than query. The attacked host has no way to know the location of the attacker from the attacking packets, sender of which often does not even have logging.

Transport layer protocols handling multiple addresses of a host is subject to similar attack.

If transport layer protocols handling multiple addresses of a host has DoS amplification property worse than the current Internet hosts, there will be the existing security threat of DDoS will be more serious.

1.3. New DoS Opportunity on Identification

If a host has an identification involves computationally expensive security mechanism, it can be used for DoS attack to the host.

On the current Internet, cookie is exchanged before performing the computationally expensive process, though mere holding of cookie information can be expensive operation as exemplified by TCP SYN flooding.

Cookie protection, of course, is powerless against MITM.

If transport layer protocols having new connection identification mechanism does not support initial cookie exchange, there will be a new security threat of DoS.

1.4. Privacy on Identification

If transport layer protocols having new connection identification requires hosts having persisting identification information, it will be used to track the identify of the host, which is a new security threat.

2. Author's Address

Masataka Ohta
Graduate School of Information Science and Engineering
Tokyo Institute of Technology
2-12-1, O-okayama, Meguro-ku, Tokyo 152-8552, JAPAN

Phone: +81-3-5734-3299
Fax: +81-3-5734-3299
EMail: mohta@necom830.hpcl.titech.ac.jp