Independent Submission
Request for Comments: 6978
Category: Experimental
ISSN: 2070-1721

J. Touch
USC/ISI

July 2013

A TCP Authentication Option Extension for NAT Traversal

Abstract

This document describes an extension to the TCP Authentication Option (TCP-AO) to support its use over connections that pass through Network Address Translators and/or Network Address and Port Translators (NATs/NAPTs). This extension changes the data used to compute traffic keys, but it does not alter TCP-AO's packet processing or key generation algorithms.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for examination, experimental implementation, and evaluation.

This document defines an Experimental Protocol for the Internet community. This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not a candidate for any level of Internet Standard; see 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/rfc6978.

Table of Contents

1. Introduction

This document describes an extension to the TCP Authentication Option (TCP-AO) [RFC5925] called TCP-AO-NAT to support its use in the presence of Network Address Translators and/or Network Address and Port Translators (NATs/NAPTs) [RFC2663]. These devices translate the source address and/or the source port number of a TCP connection. TCP-AO without TCP-AO-NAT extensions would be sensitive to these modifications and would discard authenticated segments.

At least one potential application of TCP-AO-NAT is to support the experimental multipath TCP protocol [RFC6824], which uses multiple IP addresses to support a single TCP transfer.

This document assumes detailed familiarity with TCP-AO [RFC5925]. As a preview, this document focuses on how TCP-AO generates traffic keys, and it does not otherwise alter the TCP-AO mechanism or that of its key generation [RFC5926].

2. Conventions Used in This Document

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]. When used in lower case, these words have their conventional meaning and do not convey the interpretations in RFC 2119.

3. Background

TCP-AO generates traffic keys that are specific to a socket pair [RFC5925]. The following information is used to create a connection's traffic keys. (Note that 'local' and 'remote' are interpreted as in TCP-AO [RFC5925].)

- IP local address
- IP remote address
- TCP local port
- TCP remote port
- TCP local Initial Sequence Number (ISN)
- TCP remote Initial Sequence Number (ISN)

Of these fields, the remote ISN is not known for SYN segments and is excluded from the traffic key used to authenticate them. Otherwise, all fields are used in the traffic keys of all other segments.

NATs and NAPTs (both referred to herein as "NATs", even if port translation is included) would interfere with these uses, because they alter the IP address and TCP port of the endpoint behind the NAT [RFC2663].

4. Extension to Allow NAT Traversal

The premise of TCP-AO-NAT is that it might be useful to allow TCP-AO use in the presence of NATs, e.g., to protect client/server communication where clients are behind NATs.

This document describes TCP-AO-NAT, an extension to TCP-AO that enables its use in the presence of NATs. This extension requires no modification to the TCP-AO header or packet processing, and it requires no modification to the algorithms used to generate traffic keys [RFC5926]. The change is limited to the data used to generate traffic keys only.

In TCP-AO, "a Master Key Tuple (MKT) describes the TCP-AO properties to be associated with one or more connections" [RFC5925]. This includes the TCP connection identifier, the TCP option flag (indicating whether TCP options other than TCP-AO are included in the

Message Authentication Code (MAC) calculation), keying information, and other parameters. TCP-AO-NAT augments the MKT with two additional flags:

- localNAT
- remoteNAT

TCP-AO implementations supporting TCP-AO-NAT MUST support both localNAT and remoteNAT flags.

These flags indicate whether a segment's local or remote (respectively) IP address and TCP port are zeroed before MAC calculation, either for creating the MAC to insert (for outgoing segments) or for calculating a MAC to validate against the value in the option. These flags modify TCP-AO processing rules as follows:

- In TCP-AO-NAT, traffic keys are computed by zeroing the local/remote IP address and TCP port as indicated by the localNAT or remoteNAT flags.
- In TCP-AO-NAT, MAC values are computed by zeroing the local/remote IP address and TCP port as indicated by the localNAT or remoteNAT flags.

The use of these flags needs to match on both ends of the connection, just as with all other MKT parameters.

5. Intended Use

A host MAY use TCP-AO-NAT when it is behind a NAT, as determined using NAT discovery techniques, or when TCP-AO protection is desired but conventional TCP-AO fails to establish connections.

A client behind a NAT MAY set localNAT=TRUE for MKTs supporting TCP-AO-NAT for outgoing connections. A server MAY set remoteNAT=TRUE for MKTs supporting TCP-AO-NAT for incoming connections. Peer-to-peer applications with dual NAT support, e.g., those traversing so-called 'symmetric NATs' [RFC5389], MAY set both localNAT=TRUE and remoteNAT=TRUE for MKTs supporting TCP-AO-NAT bidirectionally. Once these flags are set in an MKT, they affect all connections that match that MKT.

TCP-AO-NAT is intended for use only where coordinated between endpoints for connections that match the shared MKT parameters, as with all other MKT parameters.

Note that TCP-AO-NAT is not intended for use with services transiting Application Layer Gateways (ALGs), i.e., NATs that also translate in-band addresses, such as used in FTP or SIP. TCP-AO-NAT protects the contents of the TCP segments from modification and would (correctly) interpret such alterations as an attack on those contents.

6. Security Considerations

TCP-AO-NAT does not affect the security of connections that do not set either the localNAT or remoteNAT flags. Such connections are not affected themselves and are not affected by segments in other connections that set those flags.

Setting either the localNAT or remoteNAT flags reduces the randomness of the input to the Key Derivation Function (KDF) used to generate the traffic keys. The largest impact occurs when using IPv4, which reduces the randomness from 2 IPv4 addresses, 2 ISNs, and both ports down to just the two ISNs when both flags are set. The amount of randomness in the IPv4 addresses and service port is likely to be small, and the randomness of the dynamic port is under debate and should not be considered substantial [RFC6056]. The KDF input randomness is thus expected to be dominated by that of the ISNs, so reducing it by either or both of the IPv4 addresses and ports is not expected to have a significant impact.

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.

[RFC5925] Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option", RFC 5925, June 2010.

7.2. Informative References

[RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

[RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", RFC 5389, October 2008.

[RFC5926] Lebovitz, G. and E. Rescorla, "Cryptographic Algorithms for the TCP Authentication Option (TCP-AO)", RFC 5926, June 2010.

[RFC6056] Larsen, M. and F. Gont, "Recommendations for Transport-Protocol Port Randomization", BCP 156, RFC 6056, January 2011.

[RFC6824] Ford, A., Raiciu, C., Handley, M., and O. Bonaventure, "TCP Extensions for Multipath Operation with Multiple Addresses", RFC 6824, January 2013.

8. Acknowledgments

This extension was inspired by discussions with Dan Wing.

This document was initially prepared using 2-Word-v2.0.template.dot.

Author's Address

Joe Touch
USC/ISI
4676 Admiralty Way
Marina del Rey, CA 90292
USA

Phone: +1 (310) 448-9151
EMail: touch@isi.edu