Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 18, 2007

S. Bellovin
Columbia University
October 15, 2006

# Towards a TCP Security Option
## draft-bellovin-tcpsec-00.txt

## Status of this Memo



## Copyright Notice



## Abstract

The TCP-MD5 option, commonly used to secure BGP sessions between routers, has many serious deficiencies. We present here justifications for designing a new, more capable version of that option; we also discuss some of the design criteria for one.

## 1. Introduction

Putting a security service into the transport layer has a long history. SP4 [SP4] [SP4P] provided that service for the Secure Data Network System (SDNS); OSI incorporated SP4 into its protocol suite as the Transport Layer Security Protocol (TLSP) [TLSP].

TCP/IP has not had a full-fledged equivalent, though the TCP-MD5 option [RFC2385] has served some of its purposes. In this memo, we analyze the problem and discuss what a solution should look like,

Note that we have deliberately used the phrase "security service". Both a confidentiality and an authentication-only service have their place. This memo is agnostic on that point, though we note that TCP-MD5 is authentication-only.

## 2. Motivation

It is quite clear that the existing TCP authentication option [RFC2385] is inadequate. It is cryptographically unsound, requiring a process waiver to permit its continued use with BGP [RFC4278]. It has no key identification field, necessitating a heuristic for key change [I-D.bellovin-keyroll2385]. And it has no provision for automated key management [RFC4107], leading to the problems described in [RFC3562].

What is less clear is why authentication is needed at all at the TCP layer. IPsec [RFC4301] can protect the entire TCP header and payload, though with help from the kernel or outboard hardware; TLS [RFC4346] can protect any the payload of TCP connection, after changes to the application. That said, these existing solutions have further deficiencies.

The most serious problem with IPsec is that it is hard to protect an individual application with it [I-D.bellovin-useipsec]. Put briefly, IPsec operates at the IP layer (with a sprinkling of transport layer concepts, such as port numbers, for additional flavor). It also has problems with NAT traversal [RFC2709] [RFC3715] [RFC3947] [RFC3948]: NAT boxes can neither examine nor modify port numbers on most IPsec-protected traffic, which causes very real problems in many environments (though not, admittedly, when protecting BGP). The net result is that IPsec usage is largely limited to virtual private

network scenarios; it is rarely used or usable for individual applications.

To be sure, BGP speakers will rarely, if ever, be behind NATs. Other uses have been suggested for devices that need to look at and even





modify parts of the TCP header in ways barred by IPsec; typically, these are intended to deal with link type-specific performance issues as are seen with geostationary satellites or lossy wireless links. While it is not clear that a TCP security option can permit, say, ACK spoofing or modifications to the advertised window size without creating serious security or denial of service risks, there is sufficient demand for such facilities that the problem should at least be investigated. [[get citations]]

IPsec has often been criticized for its interference with firewalls and with traffic engineering, because it hides port numbers and flags. A TCP security option could choose to expose such fields for examination.

TLS does not suffer from any of these flaws; however, it poses issues of its own. It has integrated key management; while this works well in many environments, it is too heavy-weight or otherwise inappropriate for others. A more serious issue is the limited scope of protection provided by TLS. It operates strictly above TCP; it thus provides no protection at all against attacks against the TCP header itself. Even if TLS is in use, it is thus possible for attackers to reset connections (US-CERT Advisory TA04-111A) or perpetrate other mischief [I-D.ietf-tcpm-tcp-antispoof].

It is clear, then, that some intermediate protection mechanism can be justfied. While we do not propose a specific design here (nor are we convinced that there is a strong-enough market demand for general adoption of such a scheme), we believe that the question is worthy of more exploration and discussion.

## 3. Requirements for a New Option

We note here several requirements for a future TCP security option. More details may be found in [I-D.bellovin-keyroll2385].
1. It must provide protection for crucial elements of the TCP

header, including the flags field. Further details (including, for example, coverage of TCP options) are not specified here.

2. A proper cryptographic algorithm should be used, rather than an ad hoc keyed hash design.
3. The option should contain some form of key identifier field to be used for intraconnection rekeying. This field points to a receiver data structure entry that contains the actual key, much like an IPsec SPI (Security Parameter Index). (Often, the data structure will also contain auxiliary information, such as an algorithm type, but we are not prescribing any particular design here.)





4. An automated key management scheme should be defined or identified.

## 4. Security Considerations

This memo per se does not raise any non-trivial security considerations. However, any protocol designed or used to meet its requirements will need a security analysis.

## 5. References

### 5.1. Normative

[RFC2385] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, August 1998.

[RFC3562] Leech, M., "Key Management Considerations for the TCP MD5 Signature Option", RFC 3562, July 2003.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

### 5.2. Informative

[I-D.bellovin-keyroll2385]
Bellovin, S., "Key Change Strategies for TCP-MD5", draft-bellovin-keyroll2385-01 (work in progress), July 2006.

[I-D.bellovin-useipsec]
Bellovin, S., "Guidelines for Mandating the Use of IPsec", draft-bellovin-useipsec-04 (work in progress), September 2005.

[I-D.ietf-tcpm-tcp-antispoof]
Touch, J., "Defending TCP Against Spoofing Attacks", draft-ietf-tcpm-tcp-antispoof-04 (work in progress), May 2006.

[RFC2709] Srisuresh, P., "Security Model with Tunnel-mode IPsec for NAT Domains", RFC 2709, October 1999.

[RFC3715] Aboba, B. and W. Dixon, "IPsec-Network Address Translation





(NAT) Compatibility Requirements", RFC 3715, March 2004.

[RFC3947] Kivinen, T., Swander, B., Huttunen, A., and V. Volpe, "Negotiation of NAT-Traversal in the IKE", RFC 3947, January 2005.

[RFC3948] Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec ESP Packets", RFC 3948, January 2005.

[RFC4107] Bellovin, S. and R. Housley, "Guidelines for Cryptographic Key Management", BCP 107, RFC 4107, June 2005.

[RFC4278] Bellovin, S. and A. Zinin, "Standards Maturity Variance Regarding the TCP MD5 Signature Option (RFC 2385) and the BGP-4 Specification", RFC 4278, January 2006.

[SP4] Dinkel, C., "Secure Data Network System (SDNS) Network, Transport, and Message Security Protocols", NISTIR 90-4250, 1990.

[SP4P] Branstad, D., Dorman, J., Housley, R., and Randall, "SP4:

A Transport Encapsulation Security Protocol",
December 1987.

Third Aerospace Security Conference Proceedings

[TLSP] "Information technology -- Telecommunications and Information Exchange Between Systems -- Transport Layer Security Protocol", ISO/IEC 10736, 1995.

## Author's Address

Steven M. Bellovin
Columbia University
1214 Amsterdam Avenue
MC 0401
New York, NY 10027
US

Phone: +1 212 939 7149
Email: bellovin@acm.org





## Full Copyright Statement

## Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

## Acknowledgment

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