Processing of IP Security/Compartment and Precedence Information by TCP
                  draft-gont-tcpm-tcp-seccomp-prec-00.txt

Abstract

   This document discusses the security and interoperability problems
   that may arise as a result of the processing of IP security/
   compartment and precedence information by TCP. Additionally, it
   formally updates RFC 793 such that these issues are mitigated.

Status of this Memo

Copyright Notice

   described in the Simplified BSD License.

Table of Contents

1. Introduction

Section 3.9 (page 71) of RFC 793 [RFC0793] states that if the IP
security/compartment and precedence of an incoming segment does not
exactly match the security/compartment in the TCB, a RST segment
should be sent, and the connection should be aborted.

   A discussion of the IP security options relevant to this section
   can be found in Section 3.13.2.12, Section 3.13.2.13, and Section
   3.13.2.14 of [RFC6274].

This certainly provides another attack vector for performing
connection-reset attacks, as an attacker could forge TCP segments
with a security/compartment that is different from that recorded in
the corresponding TCB and, as a result, the attacked connection would
be reset.

   It is interesting to note that for connections in the ESTABLISHED
   state, this check is performed after validating the TCP Sequence
   Number and checking the RST bit, but before validating the
   Acknowledgement field. Therefore, even if the stricter validation
   of the Acknowledgement field (described in Section 3.4) was
   implemented, it would not help to mitigate this attack vector.

Resetting a connection due to a change in the Precedence value could
also have a negative impact on interoperability. For example, the
packets that correspond to a TCP connection could temporarily take a
different internet path, in which some middle-box could re-mark the
Precedence field (due to administration policies at the network to be
transited). In such a scenario, an implementation following the
advice in RFC 793 would abort the connection, when the connection
would have otherwise probably survived.

While the IPv4 Type of Service field (and hence the Precedence field)
has been redefined by the Differentiated Services (DS) field
specified in RFC 2474 [RFC2474], RFC 793 [RFC0793] was never formally
updated in this respect. We note that both legacy systems that have
not been upgraded to implement the differentiated services
architecture described in RFC 2475 [RFC2475] and current
implementations that have extrapolated the discussion of the
Precedence field to the Differentiated Services field may still be
vulnerable to the connection reset vector discussed in Section 1.

Section 2 formally updates RFC 793 [RFC0793] such that these issues
are mitigated.

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].

2. Updating RFC 793

If the IP security/compartment field of an incoming TCP segment does
not match the value recorded in the corresponding TCB, TCP MUST NOT
abort the connection, but simply discard the corresponding packet.
Additionally, this whole event SHOULD be logged as a security
violation.

If the IP Differentiated Services field of an incoming TCP segment
does not match the value recorded in the corresponding TCB, TCP MUST
NOT abort the corresponding connection.

3. IANA Considerations

This document has no IANA actions. The RFC Editor is requested to
remove this section before publishing this document as an RFC.

4. Security Considerations

This document discusses the processing of the IP security/compartment
and precedence information, and the interoperability and security
implications that arise from it. It updates RFC 793 such that the
aforementioned issues are eliminated.

5. Acknowledgements

This document is based on the technical report "Security Assessment
of the Transmission Control Protocol (TCP)" [CPNI-TCP] written by
Fernando Gont on behalf of the UK CPNI.

Fernando Gont would like to thank the UK CPNI for their continued
support.

6. References

6.1. Normative References

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7,
           RFC 793, September 1981.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

                 Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black,
              "Definition of the Differentiated Services Field (DS
              Field) in the IPv4 and IPv6 Headers", RFC 2474,
              December 1998.

   [RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z.,
              and W. Weiss, "An Architecture for Differentiated
              Services", RFC 2475, December 1998.

6.2. Informative References

   [CPNI-TCP]
              Gont, F., "CPNI Technical Note 3/2009: Security Assessment
              of the Transmission Control Protocol (TCP)", 2009, <http:/
              /www.gont.com.ar/papers/
              tn-03-09-security-assessment-TCP.pdf>.

   [RFC6274] Gont, F., "Security Assessment of the Internet Protocol
              Version 4", RFC 6274, July 2011.

Author's Address

   Fernando Gont
   UTN-FRH / SI6 Networks
   Evaristo Carriego 2644
   Haedo, Provincia de Buenos Aires 1706
   Argentina

   Phone: +54 11 4650 8472
   Email: fgont@si6networks.com
   URI: http://www.si6networks.com