Network Working Group
Request for Comments: 3128
Updates: 1858
Category: Informational

I. Miller
Singularis Ltd
June 2001

Protection Against a Variant of the Tiny Fragment Attack

Status of this Memo

Copyright Notice

Abstract

This document discusses how RFC 1858 compliant filters can be vulnerable to a variant of the "Tiny Fragment Attack" described in section 3.1 of the RFC. This document describes the attack and recommends corrective action.

1. Introduction

RFC 1858 provides an excellent description of a class of attack on Internet firewalls and proposes countermeasures. However one of these countmeasures, the "Indirect Method" (section 3.2.2) is vulnerable to a combination of two of the attacks described.

The attack combines the features of the "Tiny Fragment Attack" (section 3) and the "Overlapping Fragment Attack" (section 4).

1.1 The scope of the attack

Where the filtering rules allow incoming connections to a machine AND there other ports which allow only outgoing connections on the same host, the attack allows incoming connections to the supposedly outgoing-only ports.

Note that only the initial connection message need be fragmented. Once the connection is established further traffic on it is legal. The significance of this weakness will depend on the security policy in force.

2. The Tiny Overlapping Fragment Attack

The attack typically consists of sending three fragments.

Fragment 1: (Fragment offset = 0; length >= 16)
Includes whole header and is entirely legal. Typically it describes a SYN packet initiating a new TCP connection to a port on the target host that is allowed to receive incoming connections.
e.g., Incoming connection to port 25 SMTP.

Fragment 2: (Fragment offset = 0; length = 8)
Is only the first 8 bytes and could be legal depending on the other 8-bytes of the header, but is NOT legal combined with the corresponding bytes from Fragment 1. Such a fragment includes only the port numbers and sequence number from the TCP header. Typically this packet replaces the destination port number with a port number on which the destination host that is not allowed to receive incoming connections.

Fragment 3: (Fragment offset >= 2; length = rest of message)
Contains no header and completes the message. (This third fragment is not part of the attack. However Fragment 1 cannot be the complete message or it would be passed up to the application before Fragment 2 arrived so a third fragment is necessary.)

2.1 Example of the attack

Consider the following trivial set of rules for incoming packets:

No	Action	Source Port	Dest. Port	Flags	Purpose
1	Permit	>1023	SMTP	ANY	Incoming E-mail
2	Permit	>1023	ANY	Ack=1	Existing FTP data channel connections.
3	Deny	ANY	ANY	ANY	Default deny

Fragment 1: attacker(1234) -> target(SMTP) Ack=0
This is a new SMTP connection and is permitted by rule 1.

Fragment 2: attacker(1234) -> target(Telnet=23) Ack=absent
All fields present conform to rule 2, as it could be the start of an FTP packet.

Depending on the precise implementation of the fragment reassembly in the target machine's IP stack, fragment B may overwrite fragment A to produce:-

```
attacker(1234) -> target(Telnet) Ack=0
    (new telnet connection)
```

2.2 The failure of "Indirect Method"

The Indirect Method attempts to solve both Tiny Fragment and Overlapping Fragment attacks, solely by rejecting packets with FO=1. However none of the above fragments have FO=1, so none are rejected.

The failure is clear on careful reading. In section 3.2.2 "Indirect Method", RFC 1858 states:-

> The indirect method relies on the observation that when a TCP packet is fragmented so as to force "interesting" header fields out of the zero-offset fragment, there must exist a fragment with FO equal to 1.

This is normally true where the fragments are genuine fragments, generally by bona fide software, but it is simply not true that a hacker forging fragments is forced to produce an FO=1 fragment simply because (s)he has produced an 8-byte FO=0 fragment. The vulnerability flows from this false premise.

3. Countermeasures

Whereas apparently very elegant, RFC 1858's Indirect Method is not robust. In addition to blocking FO=1 packets, it is also necessary to block FO=0 that hold less than a complete header.

```
if FO=0 and PROTOCOL=TCP and TRANSPORTLEN < tmin then
        DROP PACKET
if FO=1 and PROTOCOL=TCP then
        DROP PACKET
```

4. Security Considerations

This memo is concerned entirely with the security implications of filtering fragmented IP packets.

5. Author's Address

Ian Miller
Singularis Ltd
32 Stockwell Street
Cambridge
CB1 3ND UK

Phone: +44 1223 511943
EMail: Ian_Miller@singularis.ltd.uk

6. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.