链滴

IPv4 首部中的 Evil bit

作者：Kael4

原文链接：https://ld246.com/article/1629811605214

来源网站：链滴

今天突然了解到IPv4中有一个“彩蛋”：Evil bit. 觉得很有意思所以在这里记下来。

首部结构

我们先看一下维基百科 IPv4给出的IPv4首部结构：

IPv4 header format

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags				Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															
⋮	⋮																																
60	480																																

可以看到其中有一个3位的Flags标志，flags的第一位就是我们的**Evil bit**, 第二位是DF(不分片)，第三是MF（还有分片）。

Evil bit来源

在维基百科 Evil bit中说到了**Evil bit**来源于RFC 3514, 是一个愚人节的幽默玩笑，用于指出ip数据包不是有恶意的，因为有了这个字段，所以接收方只需要检查Evil bit就可以知道数据包是否是恶意数据。

The **evil bit** is a fictional IPv4 packet header field proposed in RFC 3514, a humorous April Foos' Day RFC from 2003 authored by Steve Bellovin. The RFC recommended that the last remaining unused bit, the "Reserved Bit"^[1]^ in the IPv4 packet header, be used to indicate whether a packet had been sent with malicious intent, thus making computer security en

原文链接：IPv4 首部中的 Evil bit

ineering an easy problem – simply ignore any messages with the evil bit set and trust the rest.

当然了，都说了是愚人节玩笑了，那怎么可能有用嘛，不过倒是真的有这个字段，就是没啥用，一般客或者文章也不会提及这个字段是干嘛的。

而在RFC 3514中煞有其事地提到：

Currently-assigned values are defined as follows:

0x0 If the bit is set to 0, the packet has no evil intent. Hosts, network elements, etc., SHOULD ssume that the packet is harmless, and SHOULD NOT take any defensive measures. (We note hat this part of the spec is already implemented by many common desktop operating systems)

0x1 If the bit is set to 1, the packet has evil intent. Secure systems SHOULD try to defend the selves against such packets. Insecure systems MAY chose to crash, be penetrated, etc.

协议不冰冷

平时发现一些有意思的东西的时候，反应大多数都是 “**卧槽还有这种操作**”，又或者是“**迷惑，但不说**。

但是却很少会看到Evil bit这种带有一点恶趣味的东西，这种感觉就像忽然置身与2003年的愚人节，着设计者把这样一个“恶趣味”亲手放进去IPv4一样有意思。

也许在不久的未来，我们也可以在自己所创造的东西中，加一点毒蘑菇再加一点旧鞋跟似的加入一点意思的彩蛋进去。