Verifying RFC 6980 Implementations on varying Operating Systems

Jacky Hammer, jhammer@ernw.de
@pennylane0815

ERNW
providing security.

Agenda

- Introduction
- Setup
- Test Results
- Conclusions

Introduction

What's this about, anyway?

ERNW
providing security.

What is a Router in IPv6?

- RFC 2461: “Routers advertise their presence together with various link and Internet parameters either periodically, or in response to a Router Solicitation message”.

- At the end of the day, an IPv6 a router is not just a forwarding device but a provisioning system as well.

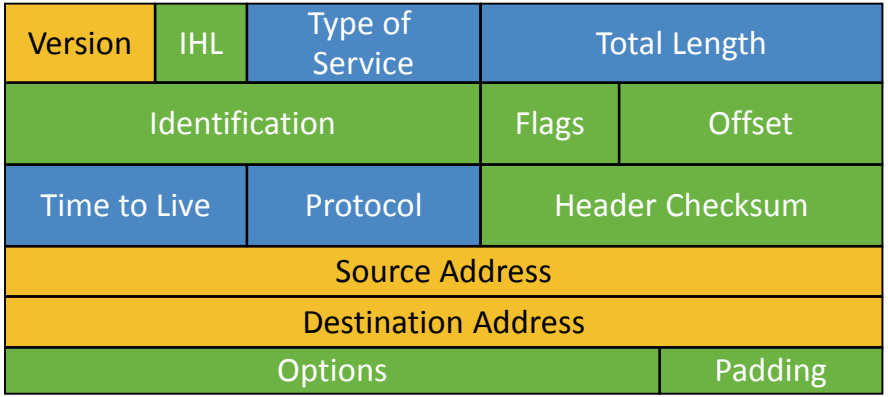
ERNW
providing security.

The Rogue Router Advertisement Problem

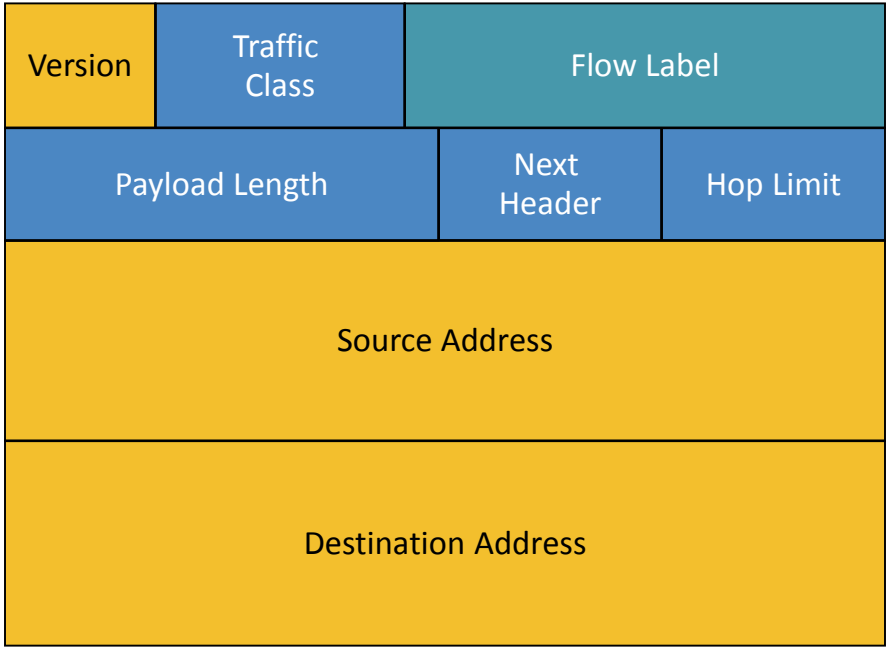
- Router advertisements are a fundamental part of “IPv6 DNA”.
  - Modifying this behavior is a severe “deviation from default” and as such “operationally expensive”
- A local link is regarded trustworthy in IPv6 world
  - All ND (including RAs) unauthenticated by default
- Attacker interferes with router discovery
  - Traffic redirection by spoofed RAs

ERNW
providing security.

IPv4 Header

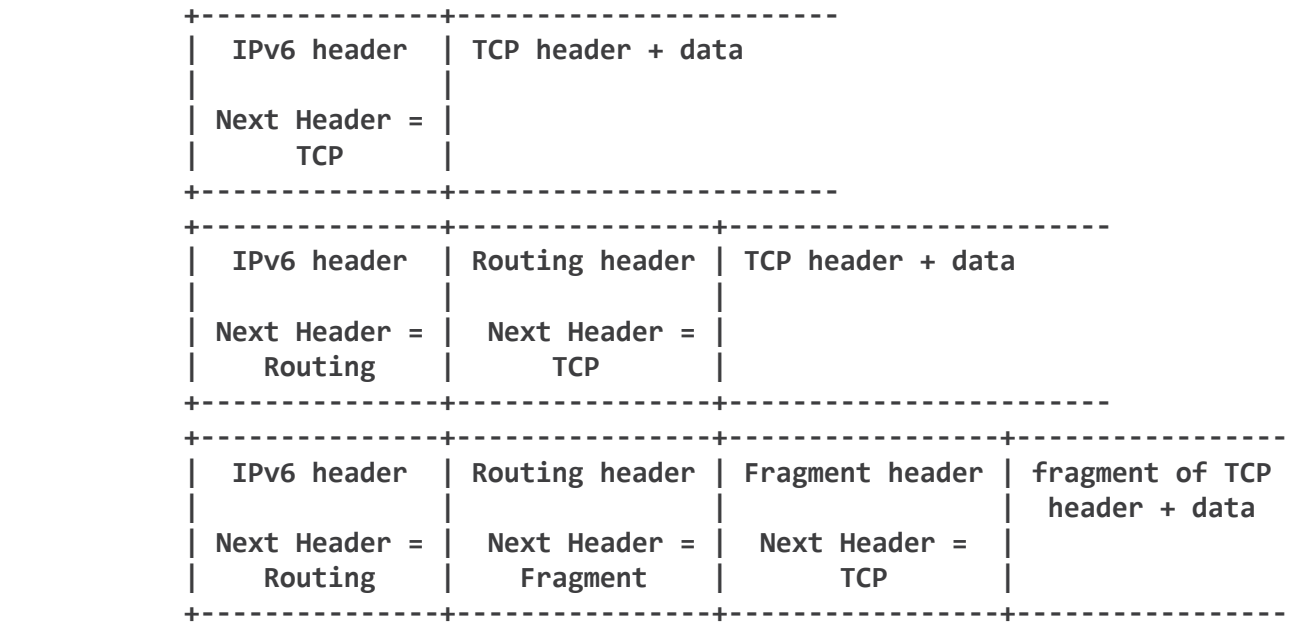


IPv6 Header



ERNW
providing security.

The Extension Header Problem



ERNW
providing security.

Interesting Extension Headers

RFC 2460

- The **Hop-by-Hop** Options header is used to carry optional information that must be examined by every node along a packet's delivery path.
- The **Routing Header** is used by an IPv6 source to list one or more intermediate nodes to be "visited" on the way to a packet's destination.
- The **Destination Options** header is used to carry optional information that need be examined only by a packet's destination node(s)

ERNW
providing security.

Neighbor Discovery (ND)

1. Neighbor Discovery / Address Resolution
2. Router Discovery
3. Prefix Discovery
4. Parameter Discovery
5. Address Autoconfiguration
6. Next-Hop Determination
7. Neighbor Unreachability Detection
8. Duplicate Address Detection
9. Redirects

RFC 6980

Internet Engineering Task Force (IETF) F. Gont
Request for Comments: 6980 SI6 Networks / UTN-FRH
Updates: 3971, 4861 August 2013
Category: Standards Track
ISSN: 2070-1721

Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery

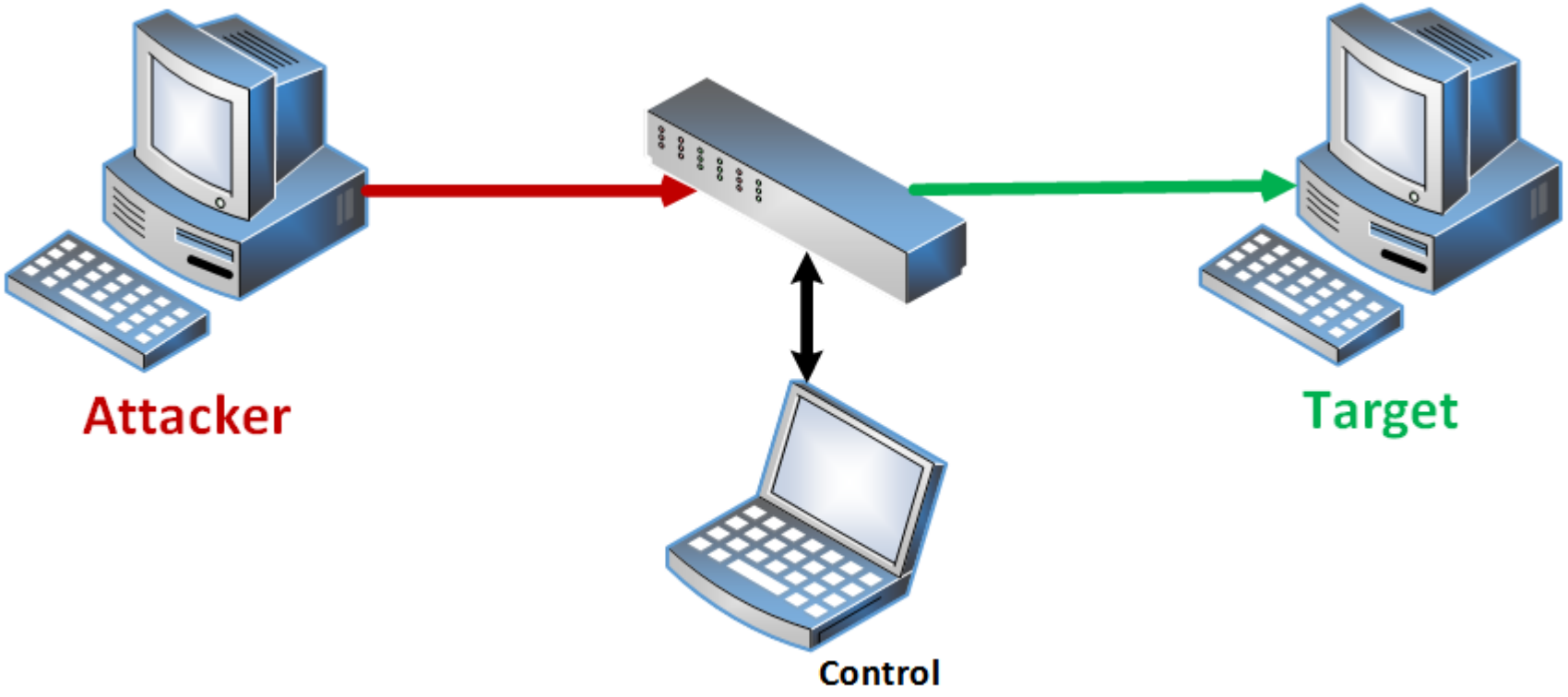
Abstract

This document analyzes the security implications of employing IPv6 fragmentation with Neighbor Discovery (ND) messages. It updates RFC 4861 such that use of the IPv6 Fragmentation Header is forbidden in all Neighbor Discovery messages, thus allowing for simple and effective countermeasures for Neighbor Discovery attacks. Finally, it discusses the security implications of using IPv6 fragmentation with SEcure Neighbor Discovery (SEND) and formally updates RFC 3971 to provide advice regarding how the aforementioned security implications can be mitigated.

The Lab Setup

What did we do - and why?

ERNW
providing security.



ERNW
providing security.

Toolkit

- Cisco Catalyst 3560 firmware version 15.2(2)E4
- TCPdump && Wireshark
- Chiron
  - For injection of fake RAs
  - by Antonios Atlasis [www.secfu.net]

```
./chiron_local_link.py enp0s25 \
      -ra \
      -pr 2001:db8:10:50:: \
      -pr-length 64 \
      -mtu 1400 \
      -s fe80::ee9a:74ff:fef5:a385
```

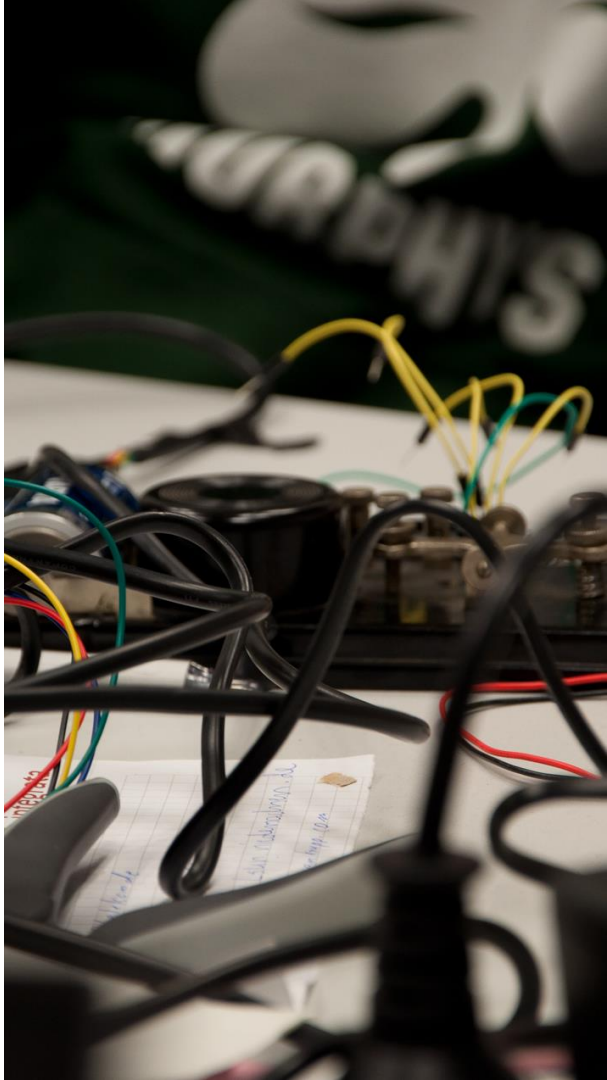
Executed Tests

- Baseline RA
  - Plain RA, unfragmented, no Extension Headers
- Unfragmented RA
  - Destination Option and/or HBH Headers
- Fragmented RAs
  - Two, three or four fragments
  - HBH, DestOpt and/or RoutingHdr in unfragmentable part
  - HBH, DestOpt and/or RoutingHdr in fragmentable part

ERNW
providing security.

Tested Systems

- Arch Linux 171101
- CentOS 7
- Debian 9
- FreeBSD 10.3
- FreeBSD 11
- OpenSUSE Leap 42.3
- Ubuntu Server 16.04 LTS
- Ubuntu Server 17.10
- Windows Server 2016 (preceeding work)

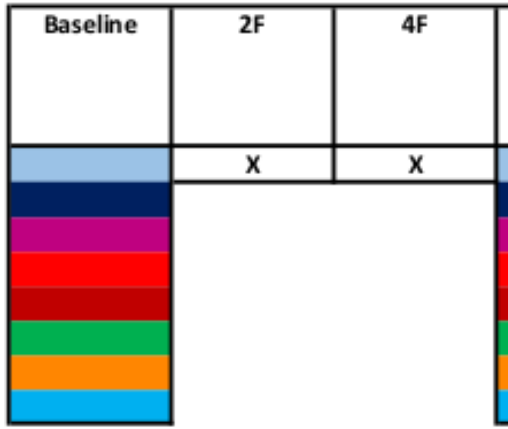


Test Results

Let’s see how that looks …

First Tests

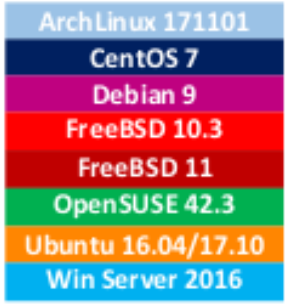
Baseline	2F	4F	NoF 1 DestOpt	NoF 1 HBH 1 DestOpt	2F 1 DestOpt in uF	2F 1 HBH 1 DestOpt in uF	2F 1 HBH 2 DestOpt in uF
	X	X			X	X	X



- ArchLinux 171101
- CentOS 7
- Debian 9
- FreeBSD 10.3
- FreeBSD 11
- OpenSUSE 42.3
- Ubuntu 16.04/17.10
- Win Server 2016

ERNW
providing security.

Let's get creative!



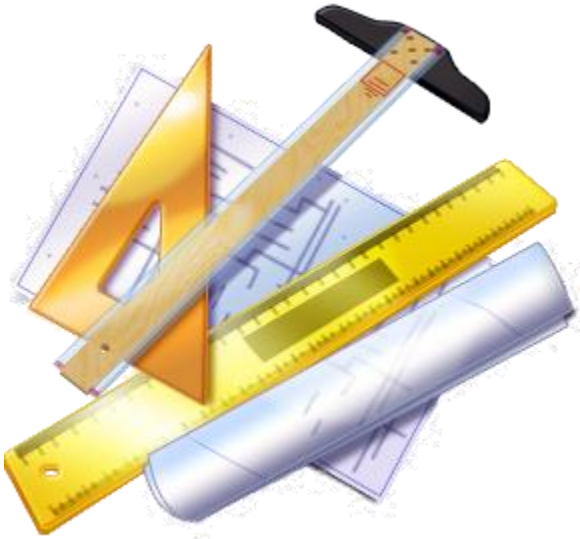
Detailed Wireshark Observations
(FreeBSD Example)

- All packets can be observed on both ends
  - Confirming successful transmission and reception
- RAs where the Hop-by-Hop header is placed after a Destination Option are discarded as of RFC 2460
  - HBH header must be first in chain
- Destination Options in fragmented RAs are evaluated by some of the Operating Systems
  - RFC 6980 seemingly not implemented correctly

ERNW
providing security.

Anything we can do about it?

- RFC 6105 proposes “IPv6 Router Advertisement Guard”
- RFC 7113 update on “Implementation Advice”
- Most current switching hardware supports that mechanism
  - Cisco: `ipv6 nd raguard`



ERNW
providing security.

Test Results with RA guard

Baseline	2F	4F	NoF 1 DestOpt	NoF 1 HBH 1 DestOpt	2F 1 DestOpt in uF	2F 1 HBH 1 DestOpt in uF	2F 1 HBH 2 DestOpt in uF
X	X	X	X	X	X	X	X

- Arch Linux 171101
- CentOS 7
- Debian 9
- FreeBSD 10.3
- FreeBSD 11
- OpenSUSE 42.3
- Ubuntu 16.04/17.10
- Win Server 2016

ERNW
providing security.

But what's that?

2F 1 DestOpt in F	2F 1 RtgHdr in F	2F 2 DestOpt in F	4F 2 DestOpt in F	2F 2 RtgHdr in F	2F 2 RtgHdr 2 DestOpt mixed	4F 2 RtgHdr 2 DestOpt mixed	3F 2 RtgHdr 2 DestOpt mixed
X	X	X		X	X	X	

ArchLinux 171101
CentOS 7
Debian 9
FreeBSD 10.3
FreeBSD 11
OpenSUSE 42.3
Ubuntu 16.04/17.10
Win Server 2016

ERNW
providing security.

Detailed Wireshark Observations
(FreeBSD Example)

- Tests with complete or fragmented RAs and Extension Headers in unfragmentable part:
  - No packet can be captured in Wireshark
  - All fragments are dropped
- Tests where Extension Headers are placed in fragmentable part:
  - All fragments (but no RA) can be observed in Wireshark
  - Only the main RA (first packet) is dropped
  - These shouldn't be, but obviously are evaluated in some cases

Conclusion

What cannot be unseen …

ERNW
providing security.

Conclusions 1/2

- Do the various Operating Systems implement RFC 6980 correctly?
- Some of them do (or at least seem to)
  - Debian, OpenSUSE, Ubuntu
- Some of them clearly don't
  - ArchLinux, CentOS, FreeBSD, Windows

ERNW
providing security.

Conclusions 2/2

- Compliance with standards not only depends largely on operating system, but obviously varies even between versions and kernels
  - All IPv6 related behavior must be carefully evaluated and tested in each specific environment
- Security mechanisms like RA guard can be evaded and will by design of IPv6 probably never be bulletproof
- Strict implementations of specifications like RFC 6980 conflicts with the Robustness Principle:
  - “Be conservative in what you do, be liberal in what you accept from others.” (Jon Postel, RFC 761)

ERNW
providing security.

Follow Ups

Coming soon on
insinuator.net

ERNW
providing security.

Thank you for your attention!

Any questions?

jhammer@ernw.de
www.ernw.de
@pennylane0815
www.insinuator.net