RFC 6980 Implementations on Different Operating Systems

Jacky Hammer

jhammer@ernw.de / @pennylane0815

ERNW
providing security.

Agenda

- Introduction
- Setup
- Test Results
- Conclusions

Introduction

Concerning Routers

ERNW
providing security.

Router Role 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”.

- In IPv6 , a router is not just a forwarding device but a provisioning system as well.

ERNW
providing security.

About Router Advertisements

- Neighbor Discovery is a fundamental part of “IPv6 DNA”.
  - Router Advertisements are an integral part of that
- 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.

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

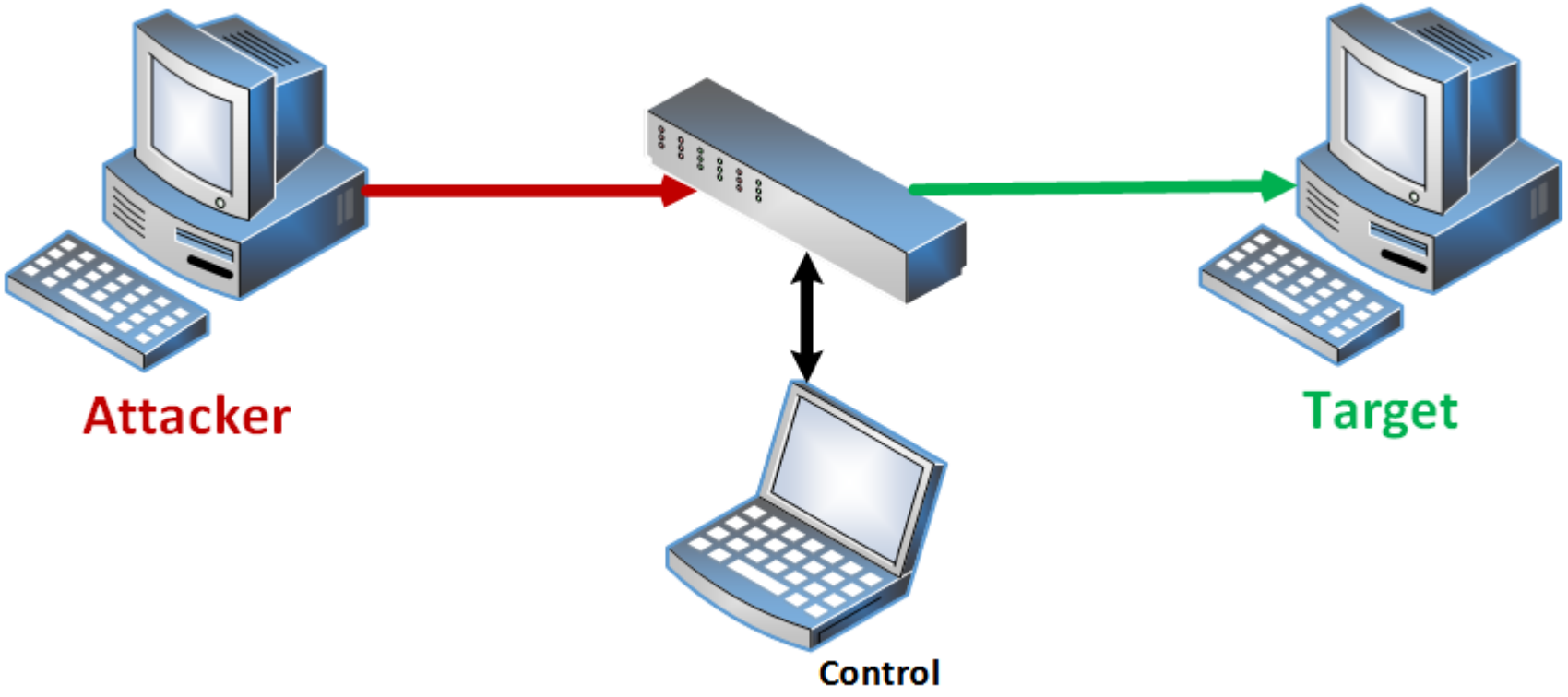
Abstract

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

Basic Parameters and Environment

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
```

ERNW
providing security.

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
  - Hop By Hop, Destination Options and/or Routing Headers in fragmentable part
  - Hop By Hop, Destination Options and/or Routing Headers in unfragmentable part

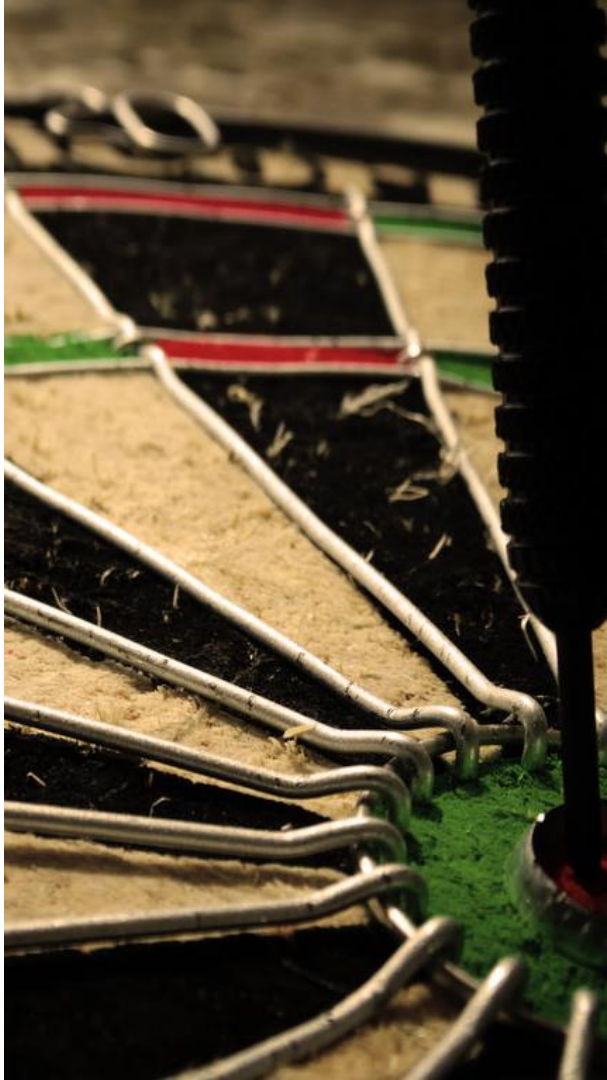
Test Results

Initial Testing on Windows Server 2016

ERNW
providing security.

First Test

- Windows Server 2016
  - Early 2017
  - By-product of general Windows IPv6 testing
  - Very bad results -> wanted to look farther



ERNW
providing security.

First Tests on Windows Server 2016

# Fragments	1	2	4	1	1	1
Extension Headers				+ 1 DestOpt	+ 1 HBH + 1 DestOpt	+ 1 DestOpt + 1 HBH
Message Part						
✓✗	✓	✗	✗	✓	✓	✗

ERNW
providing security.

First Tests on Windows Server 2016

# Fragments	2	2	2	2	2	2
Extension Headers	+ 1 DestOpt	+ 1 HBH + 1 DestOpt	+ 1 HBH + 2 DestOpt	+ 1 DestOpt	+ 1 RtgHdr	+ 1 HBH
Message Part	U	U	U	F	F	F
✓✗	✗	✗	✗	✓	✓	✗

ERNW
providing security.

First Tests on Windows Server 2016

# Fragments	2	4	2	2	4	3
Extension Headers	+ 2 DestOpt	+ 2 DestOpt	+ 2 RtgHdr	+ 2 RtgHdr + 2 DestOpt	+ 2 RtgHdr + 2 DestOpt	+ 2 RtgHdr + 2 DestOpt
Message Part	F	F	F	F	F	F
✓✗	✓	✓	✓	✓	✗	✓

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.

First Tests on Windows Server 2016

# Fragments	1	2	4	1	1	1
Extension Headers				+ 1 DestOpt	+ 1 HBH + 1 DestOpt	+ 1 DestOpt + 1 HBH
Message Part						
✓✗	✓	✗	✗	✓	✓	✗
RA Guard enabled	✗	✗	✗	✗	✗	✗

ERNW
providing security.

First Tests on Windows Server 2016

# Fragments	2	2	2	2	2	2
Extension Headers	+ 1 DestOpt	+ 1 HBH + 1 DestOpt	+ 1 HBH + 2 DestOpt	+ 1 DestOpt	+ 1 RtgHdr	+ 1 HBH
Message Part	U	U	U	F	F	F
✓✗	✗	✗	✗	✓	✗	✗
RA Guard enabled	✗	✗	✗	✗	✗	✗

ERNW
providing security.

First Tests on Windows Server 2016

# Fragments	2	4	2	2	4	3
Extension Headers	+ 2 DestOpt	+ 2 DestOpt	+ 2 RtgHdr	+ 2 RtgHdr + 2 DestOpt	+ 2 RtgHdr + 2 DestOpt	+ 2 RtgHdr + 2 DestOpt
Message Part	F	F	F	F	F	F
✓✗	✓	✓	✓	✓	✗	✓
RA Guard enabled	✗	✓	✗	✗	✗	✓

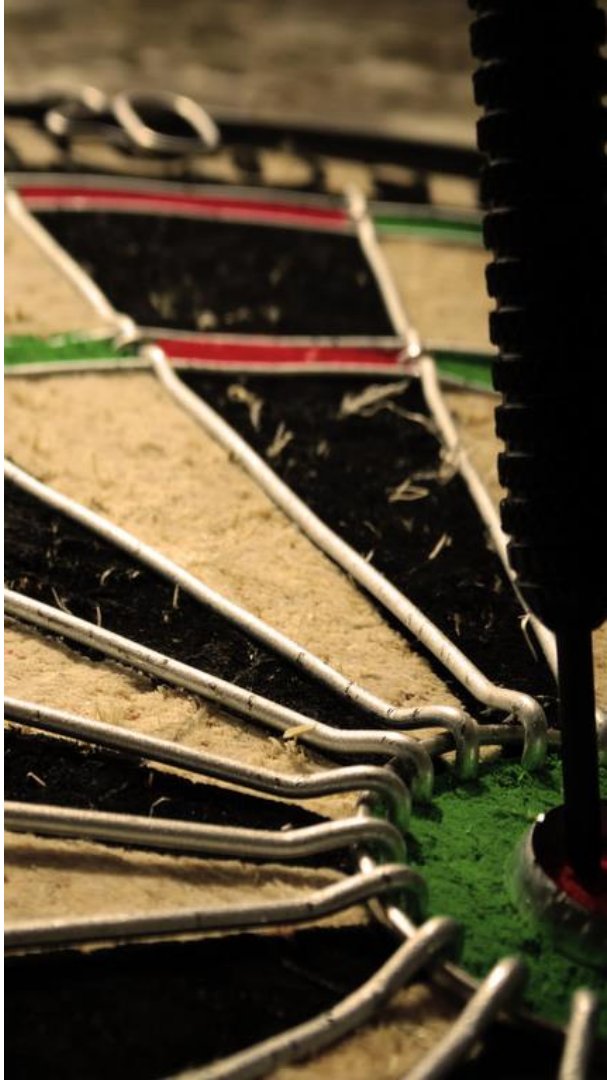
Test Results

In-depth Testing on Linux and FreeBSD Systems

ERNW
providing security.

Tested Systems (mid/late 2017)

- 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



ERNW
providing security.

Detailed Testing on Linux and BSD

(without RA Guard | with RA Guard)

# Fragments	1		2	4	1		1		1
Extension Headers					+ 1 DestOpt		+ 1 HBH + 1 DestOpt		+ 1 DestOpt + 1 HBH
Message Part									
Arch Linux 171101	✓	✗	✗	✗	✓	✗	✓	✗	✗
CentOS 7	✓	✗	✗	✗	✓	✗	✓	✗	✗
Debian 9	✓	✗	✗	✗	✓	✗	✓	✗	✗
FreeBSD 10.3	✓	✗	✗	✗	✓	✗	✓	✗	✗
FreeBSD 11.0	✓	✗	✗	✗	✓	✗	✓	✗	✗
OpenSUSE 42.3	✓	✗	✗	✗	✓	✗	✓	✗	✗
Ubuntu 16.04/17.10	✓	✗	✗	✗	✓	✗	✓	✗	✗

ERNW
providing security.

Detailed Testing on Linux and BSD

(without RA Guard | with RA Guard)

# Fragments	2	2	2	2	2	2
Extension Headers	+ 1 DestOpt	+ 1 HBH + 1 DestOpt	+ 1 HBH + 2 DestOpt	+ 1 DestOpt	+ 1 RtgHdr	+ 1 HBH
Message Part	U	U	U	F	F	F
Arch Linux 171101	✗	✗	✗	✓ ✗	✗	✗
CentOS 7	✗	✗	✗	✓ ✗	✗	✗
Debian 9	✗	✗	✗	✗	✗	✗
FreeBSD 10.3	✗	✗	✗	✓ ✗	✗	✗
FreeBSD 11.0	✗	✗	✗	✓ ✗	✗	✗
OpenSUSE 42.3	✗	✗	✗	✗	✗	✗
Ubuntu 16.04/17.10	✗	✗	✗	✗	✗	✗

ERNW
providing security.

Detailed Testing on Linux and BSD

(without RA Guard | with RA Guard)

# Fragments	2	4	2	2	4	3
Extension Headers	+ 2 DestOpt	+ 2 DestOpt	+ 2 RtgHdr	+ 2 RtgHdr + 2 DestOpt	+ 2 RtgHdr + 2 DestOpt	+ 2 RtgHdr + 2 DestOpt
Message Part	F	F	F	F	F	F
Arch Linux 171101	✓ ✗	✓ ✗	✗	✗	✗	✗
CentOS 7	✓ ✗	✓ ✗	✗	✗	✗	✗
Debian 9	✗	✗	✗	✗	✗	✗
FreeBSD 10.3	✗	✗	✗	✗	✗	✗
FreeBSD 11.0	✓ ✗	✓	✓ ✗	✓ ✗	✗	✓
OpenSUSE 42.3	✗	✗	✗	✗	✗	✗
Ubuntu 16.04/17.10	✗	✗	✗	✗	✗	✗

ERNW
providing security.

Detailed Wireshark Observations

- Without RA Guard, all RAs are correctly transmitted and received
- With RA Guard enabled, complete RAs or fragmented RAs with EHs in unfragmentable part are dropped
- With RA Guard and Extension Headers placed in fragmentable part:
  - All fragments (but no RA) can be observed in Wireshark
  - Only the main RA (first packet) is dropped
  - Should not be - but obviously are - evaluated in some cases!

First Discussions

What happened afterwards …

ERNW
providing security.

Outcomes from DENOG9 Presentation

- FreeBSD Bug 224247
  - **Summary:** [patch] RFC 6980 requires to drop fragmented IPv6 neighbour discovery
  - **Status:** Closed FIXED
  - **Version:** 11.1-STABLE
- Special thanks to Lutz!

ERNW
providing security.

Further Implications & Discussion

- High impact targets vs low-hanging fruits
  - Data Centers are high impact but more controlled environments
  - Client networks are the low-hanging fruits, thus attractive targets
  - With RA guard evasion possible, not even office nets are secure
- More targeted research on common operating systems for clients
  - Windows 10, MacOS X ?
- Research on behavior of IoT devices and mobile phones necessary

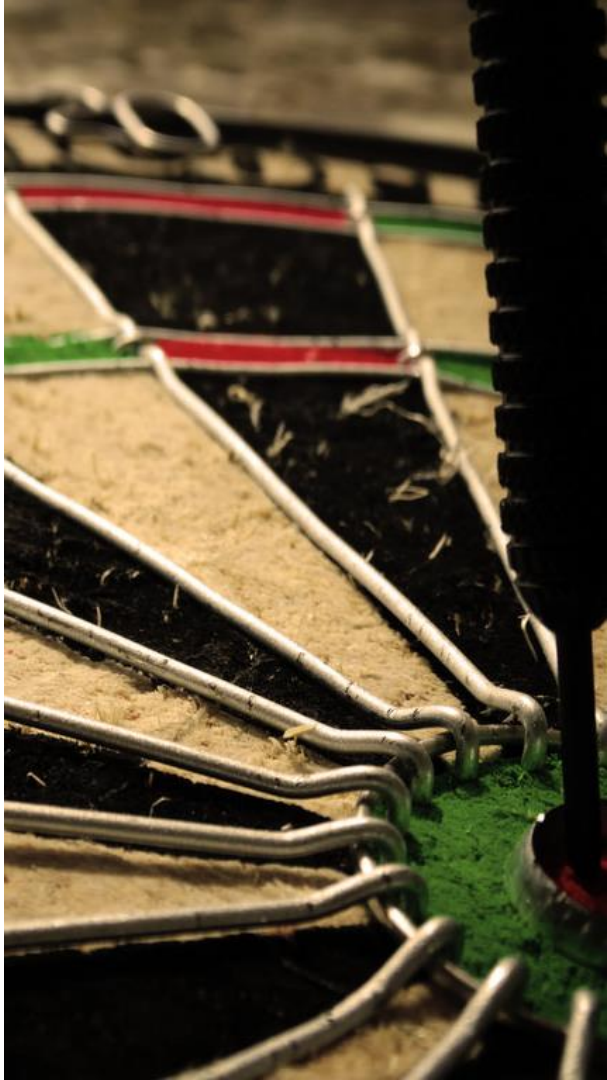
Test Results

Latest Tests on Common Client Operating Systems

ERNW
providing security.

Tested Systems (recent)

- Arch Linux (20180401)
- Debian Buster (20180424)
- FreeBSD 11.1
- Mac OS X Sierra (10.12.6)
- OpenSUSE Tumbleweed (20180420)
- Ubuntu Desktop 18.04
- Windows 10 Pro (1709)



ERNW
providing security.

Recent Testing on Common Client Operating Systems

# Fragments	1	2	4	1	1	1
Extension Headers				+ 1 DestOpt	+ 1 HBH + 1 DestOpt	+ 1 DestOpt + 1 HBH
Message Part						
Arch Linux	✓	✗	✗	✓	✓	✗
Debian Buster	✓	✗	✗	✓	✓	✗
FreeBSD 11.1	✓	✗	✗	✓	✓	✗
Mac OS X Sierra	✓	✗	✗	✓	✓	✗
OpenSUSE	✓	✗	✗	✓	✓	✗
Ubuntu 18.04	✓	✗	✗	✓	✓	✗
Windows 10 Pro	✓	✗	✗	✓	✓	✗
Windows 10 IoT Core	✓	✗	✗	✓	✓	✗

ERNW
providing security.

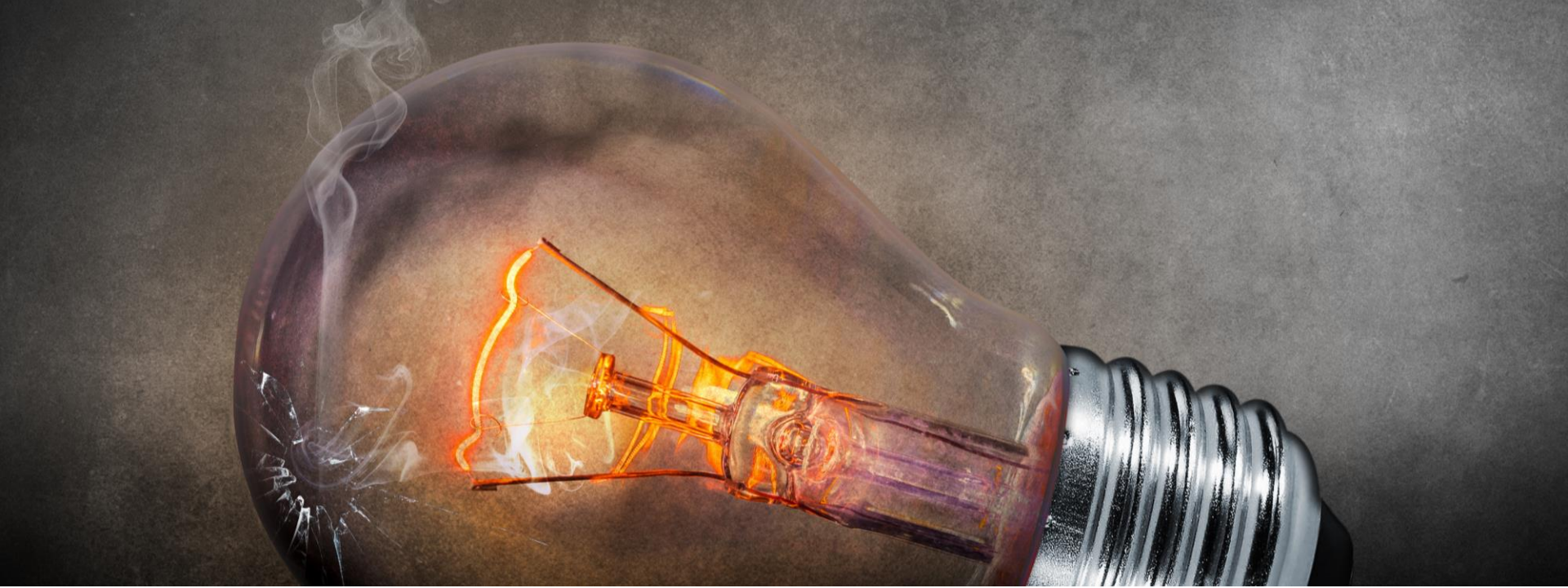
Recent Testing on Common Client Operating Systems

# Fragments	2	2	2	2	2	2
Extension Headers	+ 1 DestOpt	+ 1 HBH + 1 DestOpt	+ 1 HBH + 2 DestOpt	+ 1 DestOpt	+ 1 RtgHdr	+ 1 HBH
Message Part	U	U	U	F	F	F
Arch Linux	✗	✗	✗	✗	✗	✗
Debian Buster	✗	✗	✗	✗	✗	✗
FreeBSD 11.1	✗	✗	✗	✓	✓	✗
Mac OS X Sierra	✗	✗	✗	✗	✗	✗
OpenSUSE	✗	✗	✗	✗	✗	✗
Ubuntu 18.04	✗	✗	✗	✓	✗	✗
Windows 10 Pro	✗	✗	✗	✓	✓	✗
Windows 10 IoT Core	✗	✗	✗	✓	✓	✗

ERNW
providing security.

Recent Testing on Common Client Operating Systems

# Fragments	2	4	2	2	4	3
Extension Headers	+ 2 DestOpt	+ 2 DestOpt	+ 2 RtgHdr	+ 2 RtgHdr + 2 DestOpt	+ 2 RtgHdr + 2 DestOpt	+ 2 RtgHdr + 2 DestOpt
Message Part	F	F	F	F	F	F
Arch Linux	✗	✗	✗	✗	✗	✗
Debian Buster	✗	✗	✗	✗	✗	✗
FreeBSD 11.1	✓	✓	✓	✓	✗	✓
Mac OS X Sierra	✗	✗	✗	✗	✗	✗
OpenSUSE	✗	✗	✗	✗	✗	✗
Ubuntu 18.04	✓	✓	✗	✗	✗	✗
Windows 10 Pro	✓	✓	✓	✓	✗	✓
Windows 10 IoT Core	✓	✓	✓	✓	✗	✓



Conclusion

What cannot be unseen …

ERNW
providing security.

Conclusions

- Behavior depends not only on OS, but also on versions and kernels
  - Should be carefully evaluated and tested in each specific environment
- Security mechanisms can be evaded
  - By design of IPv6 probably impossible to be bulletproof
- Strict implementations of standards conflicts with Robustness Principle:
  - “Be conservative in what you do, be liberal in what you accept from others.” (Jon Postel, RFC 761)

ERNW
providing security.

Implications

- Users are vulnerable to rogue RAs and thus to traffic interception on the local link
  - This applies to any public, home and even office network
- We MUST NOT rely on transport layer security mechanisms like RA guard
  - Detailed datagram analysis is not possible on common network hardware
- RFC compliance MUST be tested more thoroughly by vendors and our community
- Even if standards may seem like “formalities”, they may have considerable security impacts and MUST NOT be underestimated

ERNW
providing security.

Thank you for your attention!

Any questions?

jhammer@ernw.de

www.ernw.de

@pennylane0815

www.insinuator.net