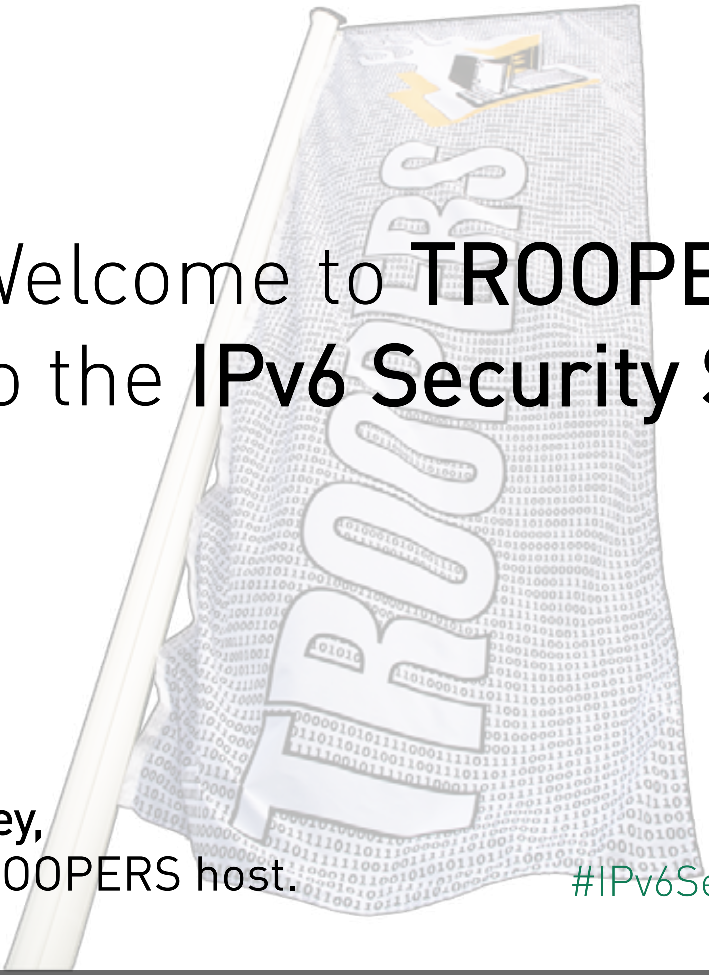
Why IPv6 Security Is So Hard

Structural Deficits of IPv6 & Their Implications

Enno Rey, erey@ernw.de

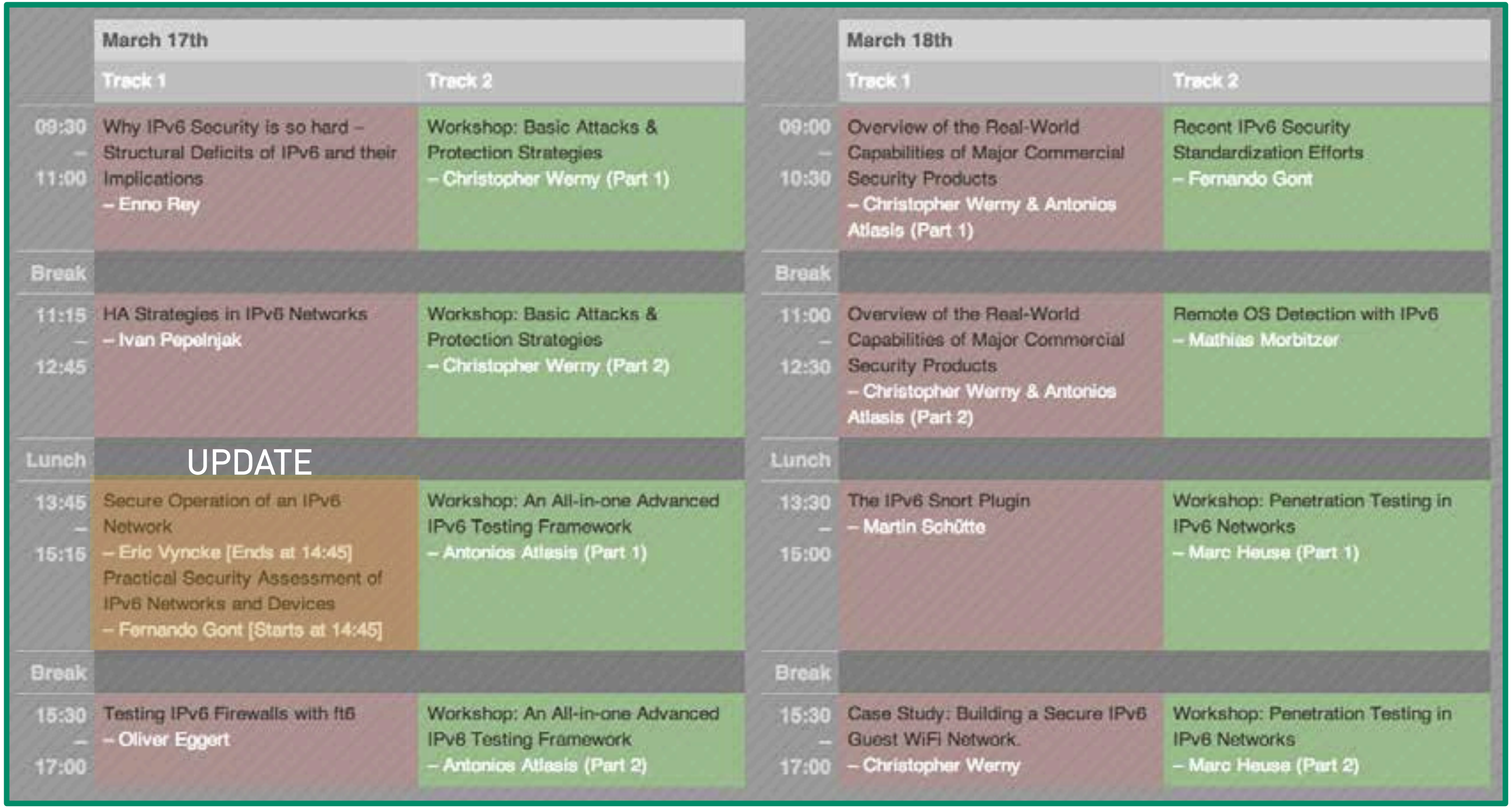


Welcome to **TROOPERS**!
Welcome to the **IPv6 Security Summit 2014**!

Enno Rey,
your TROOPERS host.

Use #TROOPERS14 or #IPv6SecSummit on Twitter to let the world know what we do here.

Agenda



	March 17th	
	Track 1	Track 2
09:30 – 11:00	Why IPv6 Security is so hard – Structural Deficits of IPv6 and their Implications – Enno Rey	Workshop: Basic Attacks & Protection Strategies – Christopher Werny (Part 1)
Break		
11:15 – 12:45	HA Strategies in IPv6 Networks – Ivan Pepelnjak	Workshop: Basic Attacks & Protection Strategies – Christopher Werny (Part 2)
Lunch	UPDATE	
13:45 – 15:15	Secure Operation of an IPv6 Network – Eric Vyncke [Ends at 14:45] Practical Security Assessment of IPv6 Networks and Devices – Fernando Gont [Starts at 14:45]	Workshop: An All-in-one Advanced IPv6 Testing Framework – Antonios Atlasis (Part 1)
Break		
15:30 – 17:00	Testing IPv6 Firewalls with ft6 – Oliver Eggert	Workshop: An All-in-one Advanced IPv6 Testing Framework – Antonios Atlasis (Part 2)

	March 18th	
	Track 1	Track 2
09:00 – 10:30	Overview of the Real-World Capabilities of Major Commercial Security Products – Christopher Werny & Antonios Atlasis (Part 1)	Recent IPv6 Security Standardization Efforts – Fernando Gont
Break		
11:00 – 12:30	Overview of the Real-World Capabilities of Major Commercial Security Products – Christopher Werny & Antonios Atlasis (Part 2)	Remote OS Detection with IPv6 – Mathias Morbitzer
Lunch		
13:30 – 15:00	The IPv6 Snort Plugin – Martin Schütte	Workshop: Penetration Testing in IPv6 Networks – Marc Heuse (Part 1)
Break		
15:30 – 17:00	Case Study: Building a Secure IPv6 Guest WiFi Network. – Christopher Werny	Workshop: Penetration Testing in IPv6 Networks – Marc Heuse (Part 2)

Some More Org Stuff

- Dinner (hosted by us) at 7 PM in restaurant "Weisser Bock" in Heidelberg old town.
  - We suggest you get there on your own. I mean spring in Heidelberg is nice.
  - We'll arrange shuttle from PMA, 6:45 PM as well.

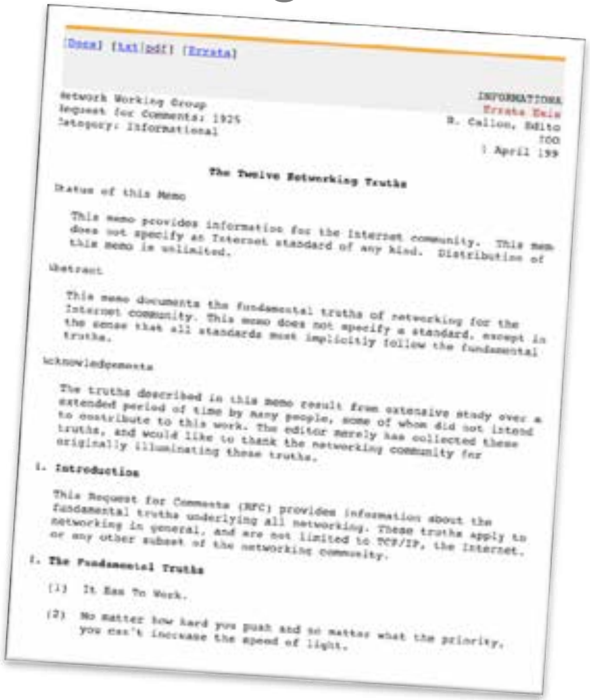
Disclaimer

- This talk is a rant ;-)
- Please note that I'm not an IPv6 sceptic
  - We do a lot IPv6 projects, on both planning/design and technical level.
  - I myself have been involved with IPv6 since 1999.
  - Given it's (already|finally) here it wouldn't help being one anyway…

Disclaimer II

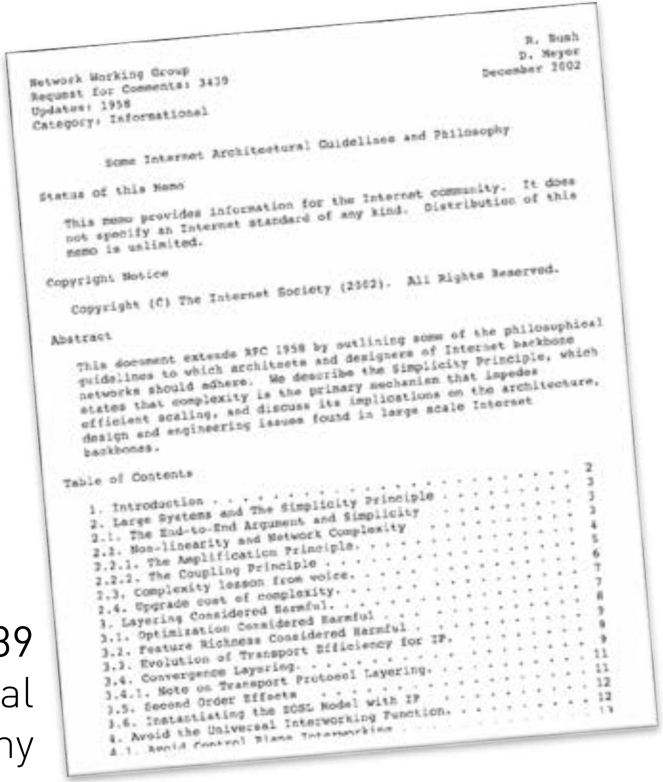
- This is probably the presentation with most (RFC) references I ever held
  - For a long time, as I hope.

The Two Most Important RFCs Ever.
I will get back on those…



```
[Docs] [txt|pdf] [Errata]

etwork Working Group                                        INFORMATIONA
equest for Comments: 1925                                    Errata Exis
ategory: Informational                                    R. Callon, Edito
                                                                      IOO
                                                              1 April 199

                    The Twelve Networking Truths

Status of this Memo

   This memo provides information for the Internet community.  This mem
   does not specify an Internet standard of any kind.  Distribution of
   this memo is unlimited.

bstract

   This memo documents the fundamental truths of networking for the
   Internet community. This memo does not specify a standard, except in
   the sense that all standards must implicitly follow the fundamental
   truths.

cknowledgements

   The truths described in this memo result from extensive study over a
   extended period of time by many people, some of whom did not intend
   to contribute to this work. The editor merely has collected these
   truths, and would like to thank the networking community for
   originally illuminating these truths.

1. Introduction

   This Request for Comments (RFC) provides information about the
   fundamental truths underlying all networking. These truths apply to
   networking in general, and are not limited to TCP/IP, the Internet,
   or any other subset of the networking community.

2. The Fundamental Truths

   (1)  It Has To Work.

   (2)  No matter how hard you push and no matter what the priority,
        you can't increase the speed of light.
```

RFC 1925
The Twelve
Networking Truths



```
                                                               R. Bush
Network Working Group                                         D. Meyer
Request for Comments: 3439                               December 2002
Updates: 1958
Category: Informational

        Some Internet Architectural Guidelines and Philosophy

Status of this Memo

   This memo provides information for the Internet community.  It does
   not specify an Internet standard of any kind.  Distribution of this
   memo is unlimited.

Copyright Notice

   Copyright (C) The Internet Society (2002).  All Rights Reserved.

Abstract

   This document extends RFC 1958 by outlining some of the philosophical
   guidelines to which architects and designers of Internet backbone
   networks should adhere.  We describe the Simplicity Principle, which
   states that complexity is the primary mechanism that impedes
   efficient scaling, and discuss its implications on the architecture,
   design and engineering issues found in large scale Internet
   backbones.

Table of Contents

   1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . .  2
   2. Large Systems and The Simplicity Principle . . . . . . . . . .  3
   2.1. The End-to-End Argument and Simplicity . . . . . . . . . . .  3
   2.2. Non-linearity and Network Complexity . . . . . . . . . . . .  3
   2.2.1. The Amplification Principle. . . . . . . . . . . . . . . .  4
   2.2.2. The Coupling Principle . . . . . . . . . . . . . . . . . .  5
   2.3. Complexity lesson from voice. . . . . . . . . . . . . . . . .  6
   2.4. Upgrade cost of complexity. . . . . . . . . . . . . . . . . .  7
   3. Layering Considered Harmful. . . . . . . . . . . . . . . . . .  7
   3.1. Optimization Considered Harmful . . . . . . . . . . . . . . .  8
   3.2. Feature Richness Considered Harmful . . . . . . . . . . . . .  9
   3.3. Evolution of Transport Efficiency for IP. . . . . . . . . . .  9
   3.4. Convergence Layering. . . . . . . . . . . . . . . . . . . . .  9
   3.4.1. Note on Transport Protocol Layering. . . . . . . . . . . . 11
   3.5. Second Order Effects  . . . . . . . . . . . . . . . . . . . . 11
   3.6. Instantiating the EOSL Model with IP  . . . . . . . . . . . . 12
   4. Avoid the Universal Interworking Function. . . . . . . . . . . 12
   4.1. Avoid Control Plane Interworking . . . . . . . . . . . . . .  13
```

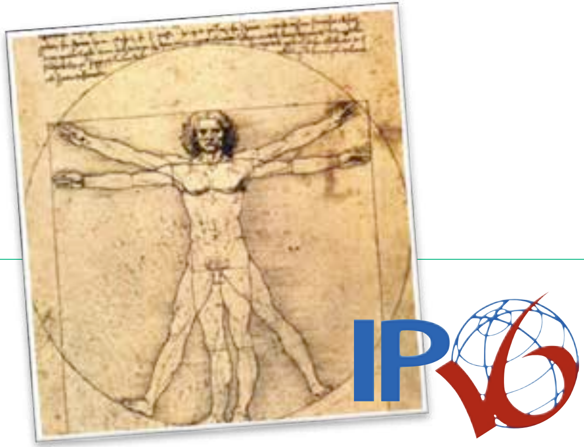
RFC 3439
Some Internet Architectural
Guidelines and Philosophy

- History

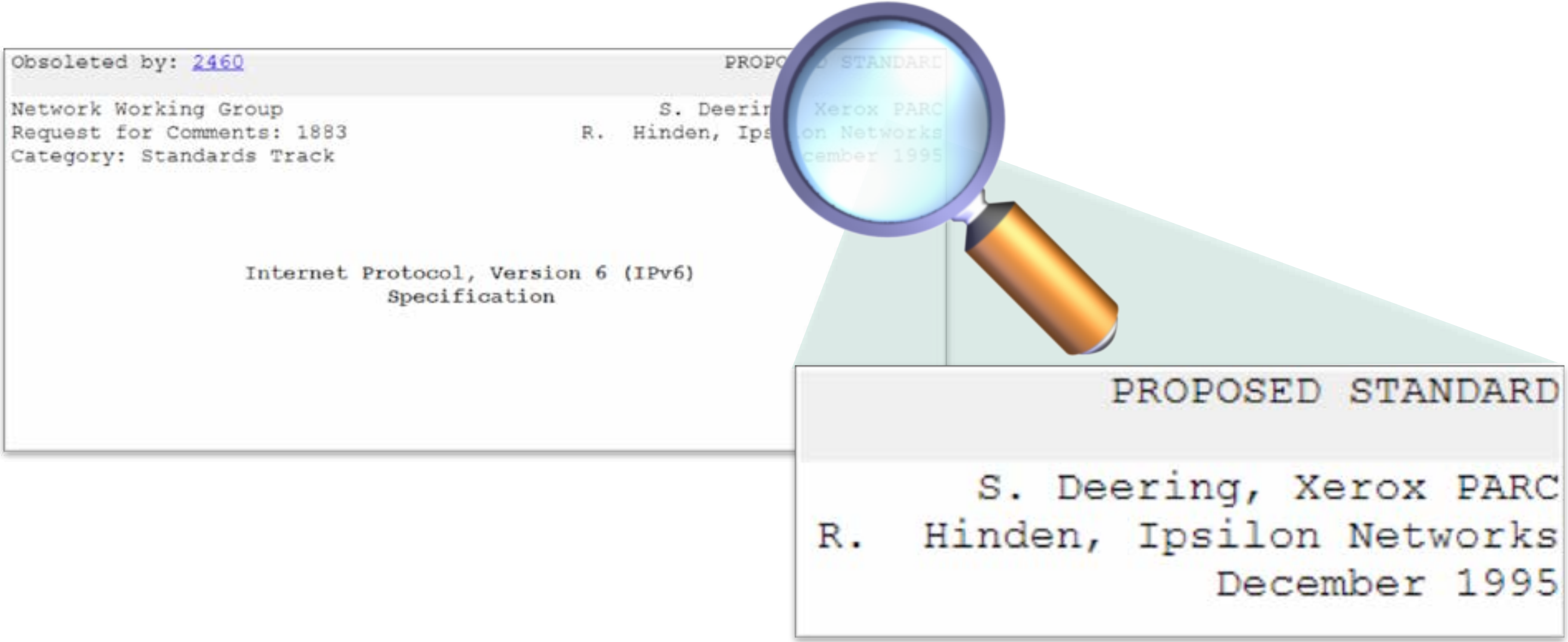
- Properties

- Impact / Interference

History



When It All Started



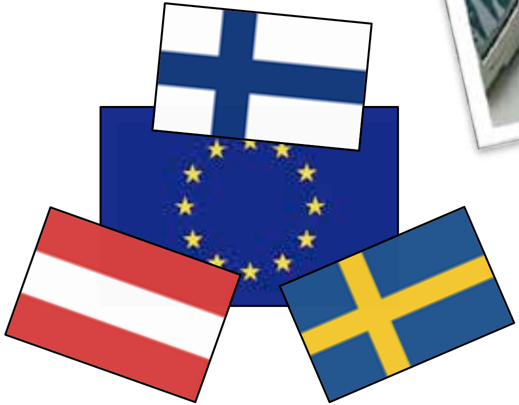
```
Obsoleted by: 2460                                       PROPOSED STANDARD

Network Working Group                                S. Deering, Xerox PARC
Request for Comments: 1883                     R.   Hinden, Ipsilon Networks
Category: Standards Track                                     December 1995


                    Internet Protocol, Version 6 (IPv6)
                               Specification
```

PROPOSED STANDARD

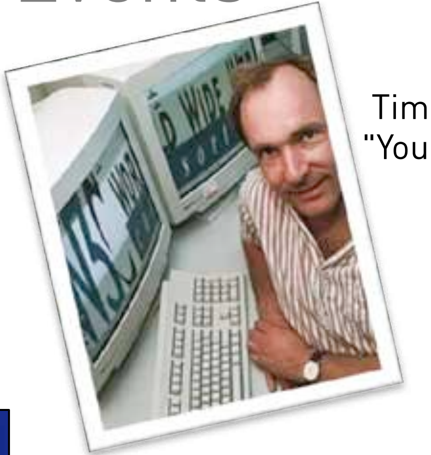
S. Deering, Xerox PARC
R.   Hinden, Ipsilon Networks
December 1995

1995 - Some Random Events

The State of Mississippi ratifies the abolition of slavery.



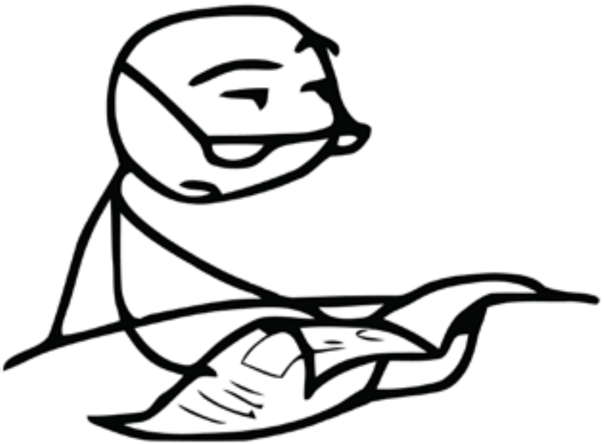
Austria, Finland & Sweden join the EU.



Tim Berners-Lee wins Kilby Foundation's "Young Innovator of the Year" award for his work on sth. called *hypertext*.

Windows 95 is released

Ok, ok, I'll Try to Be Serious



- In 1995 there was a wholly different understanding of (computer) networking and its problems.
  - Packet forwarding was mostly done in software → slow & expensive (CPU cycle wise).
  - Broadcasts considered harmful.
  - No virtualized or "mobile" networking.

- This led to certain IPv6 architecture principles...

Here's Ivan's Comments

When asked about 1995 networking

- They wanted to retain end-to-end paradigm (which got broken by NAT).
- Security was not _that_ important, L4-7 security in the network was non-existent (firewalls were usually also proxies).
- Bandwidth was _expensive_.
- Multihoming (connectivity to 2 or more ISPs) was virtually non-existent.
- They thought they can impose a worldwide hierarchical addressing scheme (like telephone system), PI addresses were given out 15+ years after IPv6 started.
  - Which, btw, highlights another aspect: IETF and registries/policing orgs. are different organizations, with potentially very different agendas…

The 90's "Crypto-Optimism"

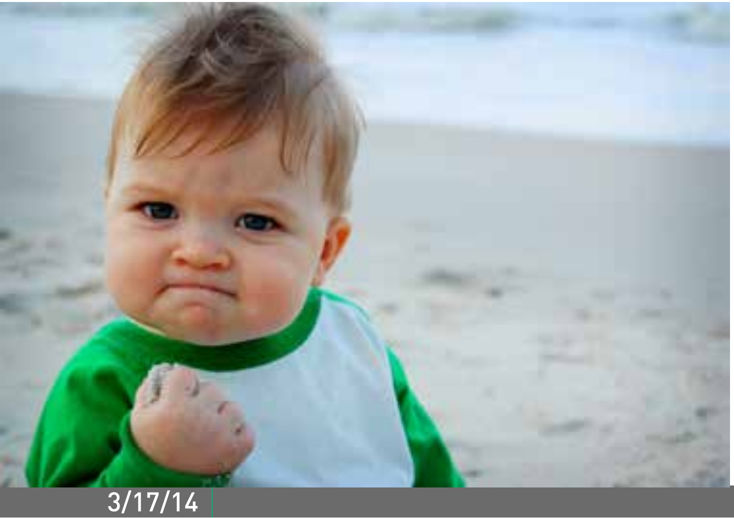
In 1995 *Clipper chip* still active.

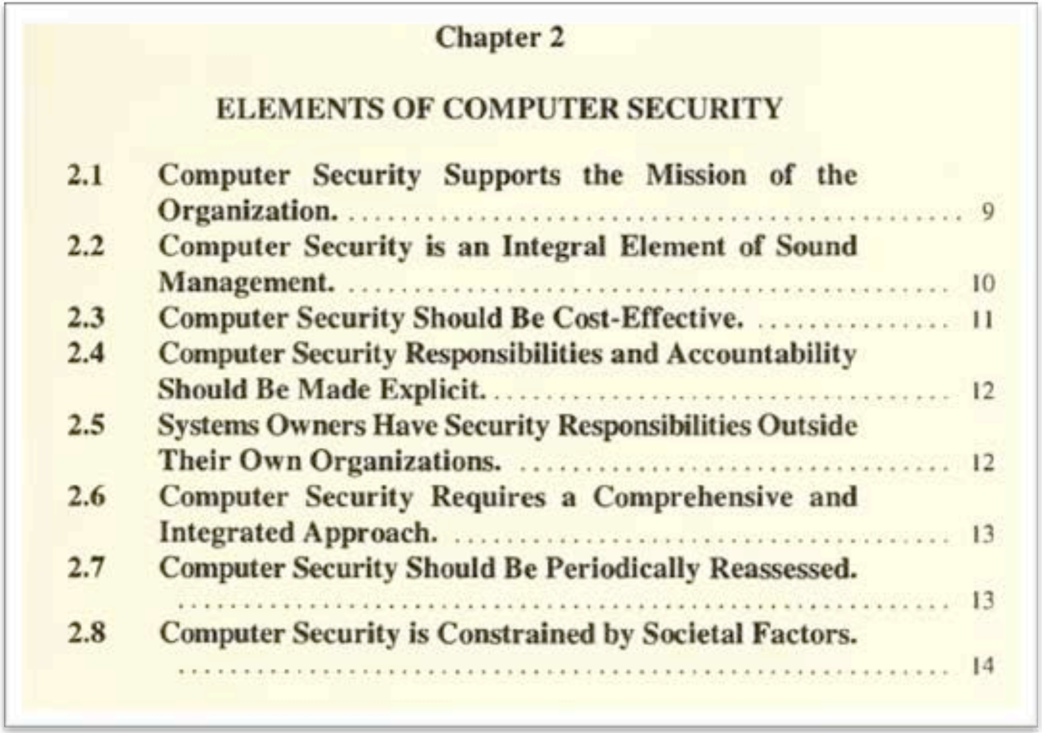
- Every network security problem considered to be solvable by means of math & some algorithms.

- This thinking shaped IPv6
  - RFC 3315 (DHCPv6) complemented by RFC 3318.
    - Which no DHCPv6 server I know of supports!
  - RFC 2461 (ND, initial spec) by RFC 3971 (SeND).
    - Which no common desktop OS I know of supports!
  - etc.

Totally Unrelated, Still...

NIST SP 800-12
An Introduction to Computer Security : The NIST Handbook

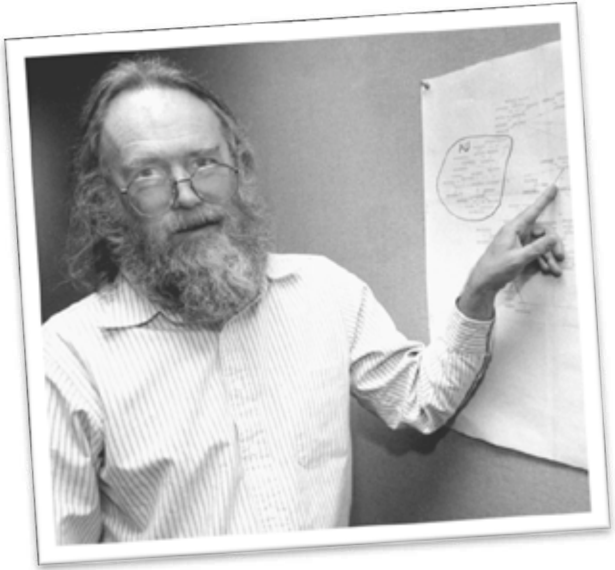




Chapter 2

ELEMENTS OF COMPUTER SECURITY

Back on Track:
The Robustness Principle



"be conservative in what you do, be liberal in what you accept from others"

RFC 761

Once Upon a Time…

Postel's law was considered beneficial.

- Don't get me wrong: I'm a big fan of the *Robustness Principle*.
  - The Internet's innovation speed strongly related to it, at the time at least.
  - Imagine ITU (or IEEE for that matter) had had to specify the Internet…
  - It's a good overall life approach as well.

- There's just one problem…

There Was a Time …

when Postel's law was considered beneficial.

- Unfortunately, it fails once an involved party deliberately plays foul.
- Or as Eric Allman states it:
  - "The Robustness Principle was formulated in an Internet of cooperators."
    - The Robustness Principle Reconsidered, 2011, http://queue.acm.org/detail.cfm?id=1999945

Wait, Humans Learn and Standards Can Be Changed! *Really?*

- Not really.
  In the IETF world standards are not withdrawn but *deprecated*.
  - Because vendors – from their perspective fully legitimately – want to protect their investments.

withdrawn

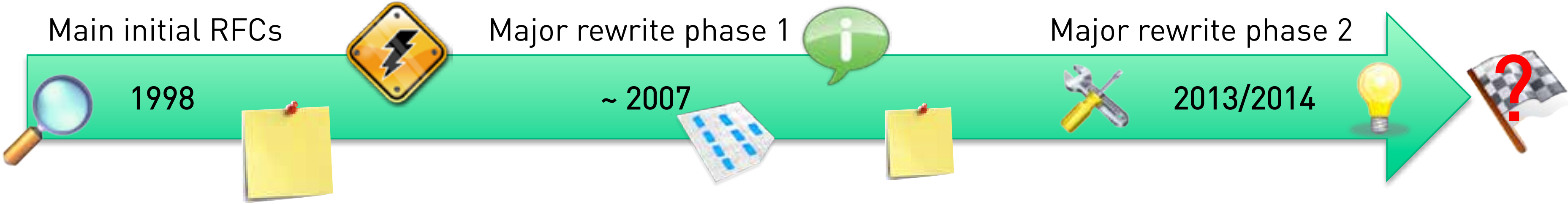
deprecated

Let’s call this “the culture of deprecation”

Culture of Deprecation & its Consequences

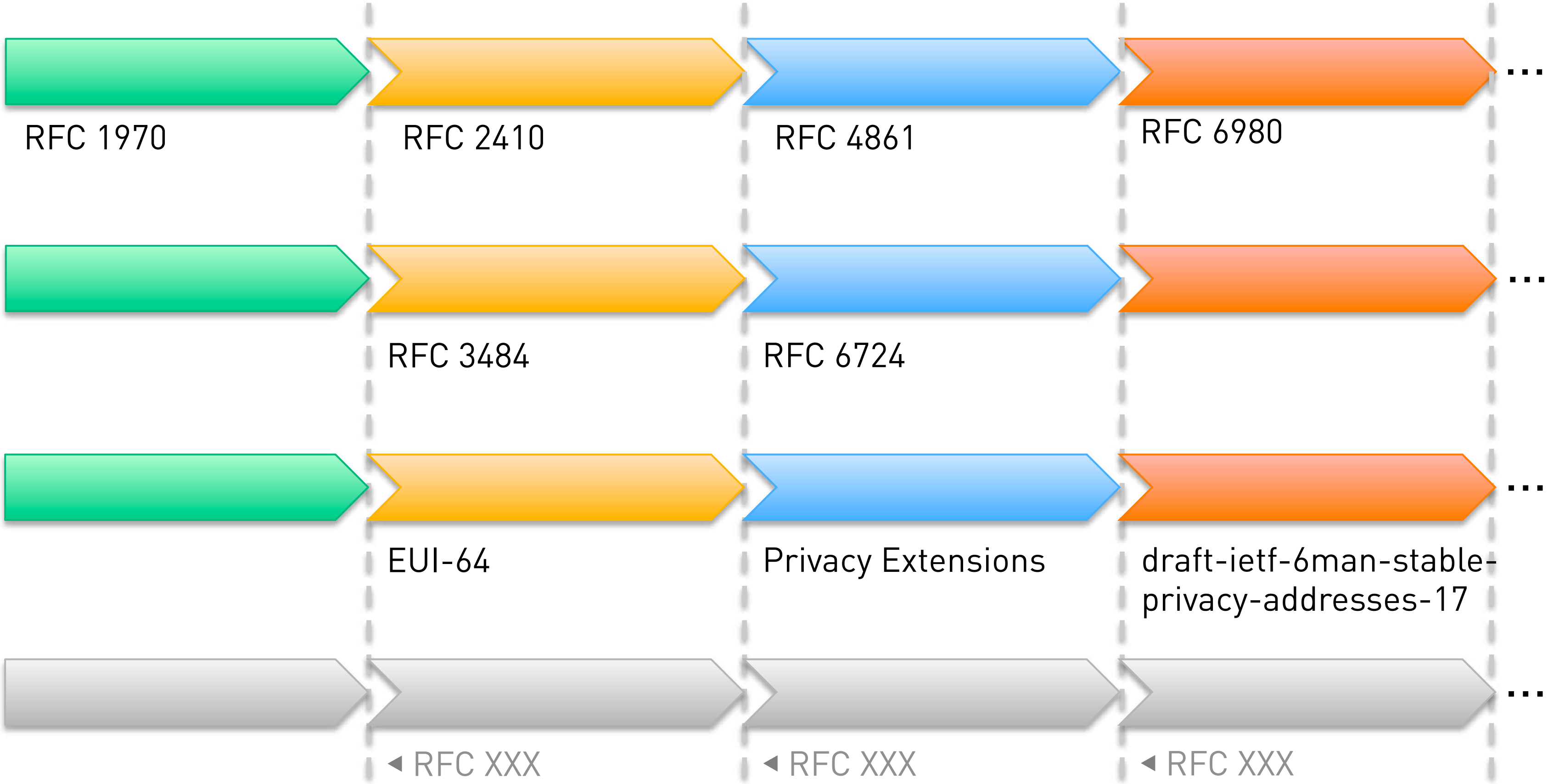
- This means that in the vast majority of IPv6 stacks around there's some remnants of $SOME_PHASE_OF_IPV6_DEVELOPMENT.
  - You thought *Routing Header 0* is long gone? Ask Antonios…
- Which in turn heavily impedes *predictability*
  - For security, predictability is certainly helpful, isn't it? ;-) More on this later.

So There's Different Generations of IPv6 Stacks



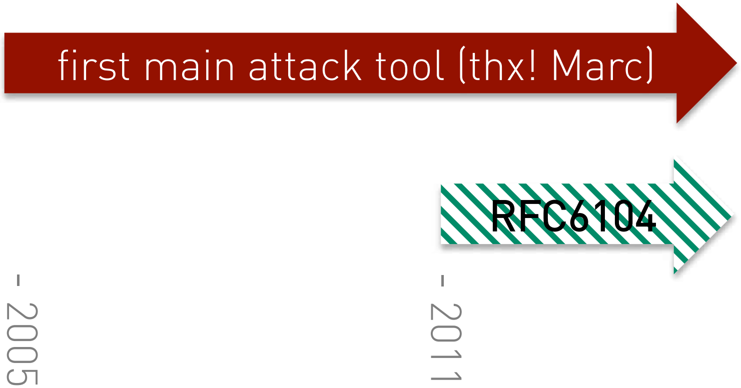
With many minor rewrites here & there…

So There's Different Generations of IPv6 Stacks



Neighbor Discovery	RFC 1970	RFC 2410	RFC 4861	RFC 6980	…
Address Selection		RFC 3484	RFC 6724		…
Generation of IID		EUI-64	Privacy Extensions	draft-ietf-6man-stable-privacy-addresses-17	…
Etc.		◀ RFC XXX	◀ RFC XXX	◀ RFC XXX	…

Talking about Time Gaps


first main attack tool (thx! Marc)

RFC6104

- 2005

- 2011

- Due to long IPv6 “warm up phase” there’s a huge asymmetry between attackers and defenders.
  - *THC-IPV6* was initially released in 2005.
  - RFC 6104 describing RA Guard is from February 2011!
    - And RA Guard still doesn’t work sufficiently. And probably never will.

Asymmetry

http://pacsec.jp/psj05/psj05-vanhauser-en.pdf

the hacker's choice

presents:

Attacking the IPv6 Protocol Suite

van Hauser, THC

vh@thc.org

http://www.thc.org

© 2005 The Hacker's Choice – http://www.thc.org – Page 1

History of #IPv6

Interim Summary

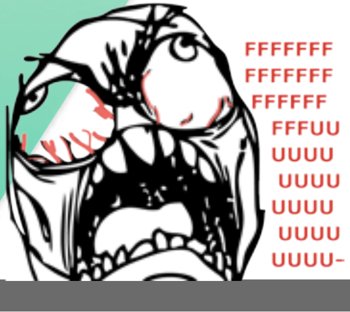
- Based on principles & design goals of a very different age.
- Since then constantly (enhanced|spoiled) by new standards & *culture of deprecation*.
- Huge asymmetry between attack & defense.

Properties

Now Let's Have a Look at Its Properties

Curtain up!

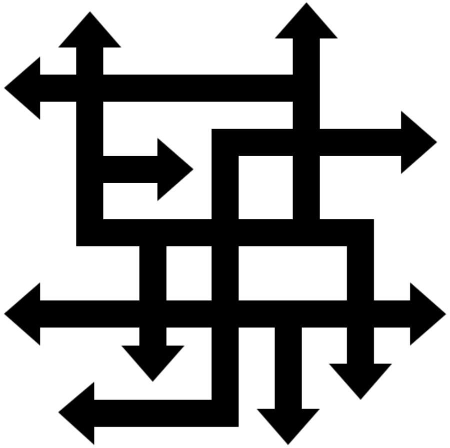
- Oh, that's an easy one. Just look at the RFCs.
- "The nice thing about standards is that you have so many to choose from."
  Andrew Tanenbaum



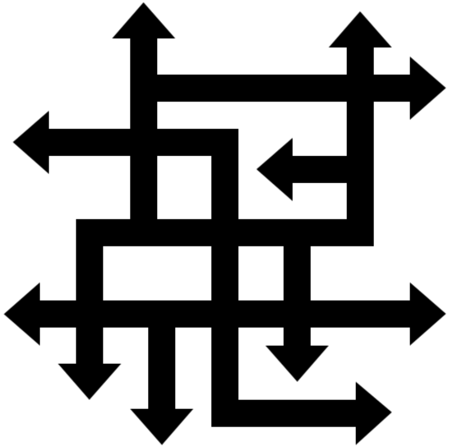
  - This was funny, wasn't it?
  - Combine this with the *culture of deprecation* and out comes… a horrible mess.

Ok, ok that Was a bit Contentious (and I keep repeating myself)

- Let's be realistic and focus on just one simple question: What's IPv6's main property?



Complexity!



Complexity

Want some samples?

"ND overspecified"

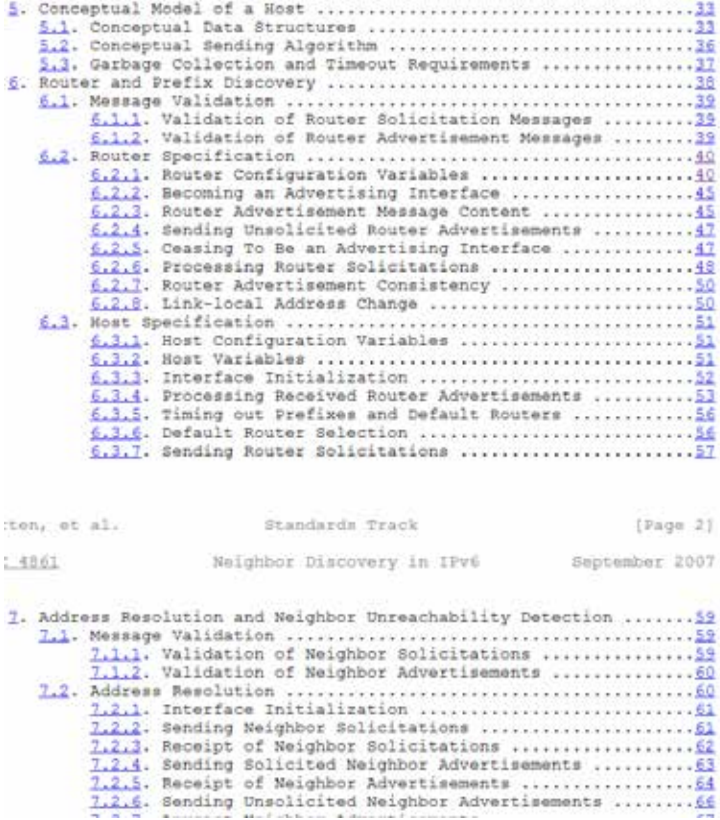
(one of the first statements in 6man at IETF 89, two weeks ago)

Neighbor Discovery

- Initial specification in RFC 1970 (Aug 1996, 82 pages), obsoleted by
- RFC 2461 (Dec 1998, 93 pages), obsoleted (after update via 4311) by
- RFC 4861 (Sep 2007, 97 pages)
  - This is mainly considered "the latest, stable one", cited in most textbooks and – if existent – stack documentation.

RFC 4861

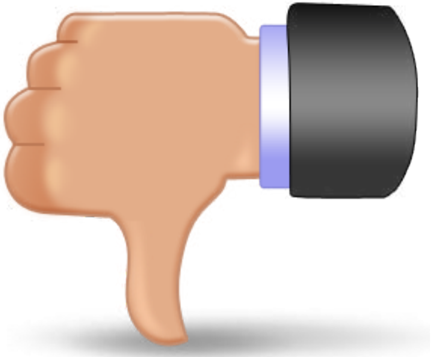
Small excerpt



ton, et al. Standards Track [Page 2]

4861 Neighbor Discovery in IPv6 September 2007

So We've Reached a kind-of stable State as for the Core of IPv6?



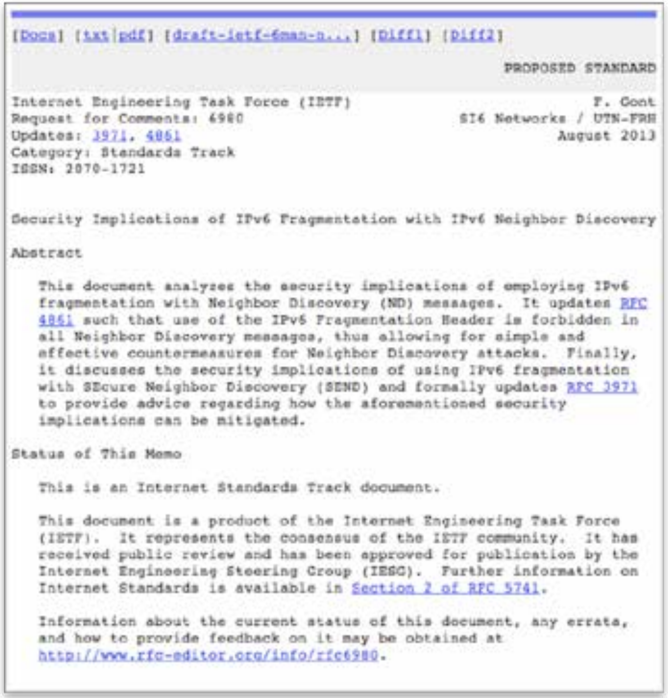
- Well… unfortunately… no.

- RFC 4861 updated by
  - RFC 5942
  - RFC 6980 *Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery*
  - *RFC 7048*
  - *yadda yadda yadda*

- Two weeks ago, at IETF 89, in *6man* (IPv6 Maintenance) and *v6ops* (IPv6 Operations) significant time spent on…

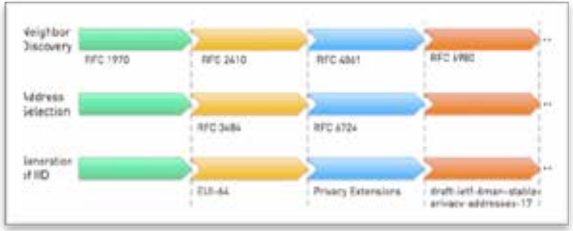
… modifications of ND!

Let’s Have a Quick Look At RFC 6980



```
[Docs] [txt|pdf] [draft-ietf-6man-n...] [Diff1] [Diff2]

                                                       PROPOSED STANDARD

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.

Status of This Memo

   This is an Internet Standards Track document.

   This document is a product of the Internet Engineering Task Force
   (IETF).  It represents the consensus of the IETF community.  It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG).  Further information on
   Internet Standards is available in Section 2 of RFC 5741.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   http://www.rfc-editor.org/info/rfc6980.
```

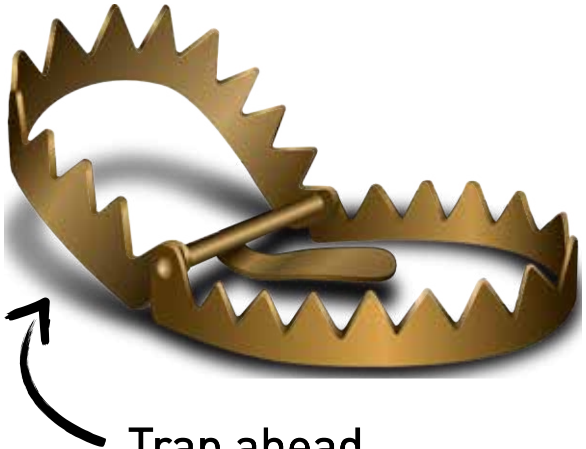
- From a security perspective this can be considered long over-due
  - Remember attack/defense asymmetry?
- Still, it adds complexity to decision taking and, subsequently, stack code.
  - And yet another sector on the time-bar.



- It doesn’t end here…
  - There’s `draft-gont-6man-lla-opt-validation-00 Validation of Neighbor Discovery Source Link-Layer Address (SLLA) and Target Link-layer Address (TLLA) options`
  - → see Fernando’s talk on standards tomorrow
  - → even more checks a stack might have to perform…

See the Relationship to The *Robustness Principle*?

Or lack thereof



Trap ahead.

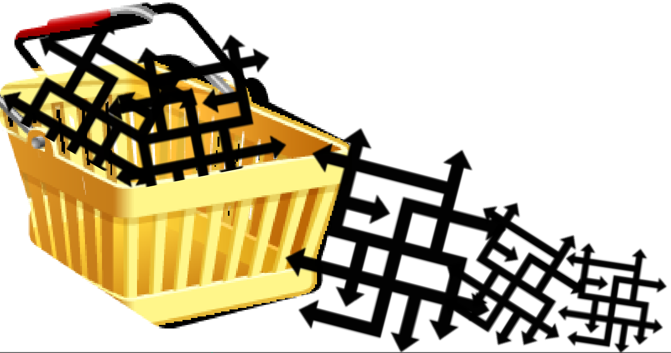
- The less we trust in the robustness principle (or, for that matter, peers on the Internet), the more checks we need.

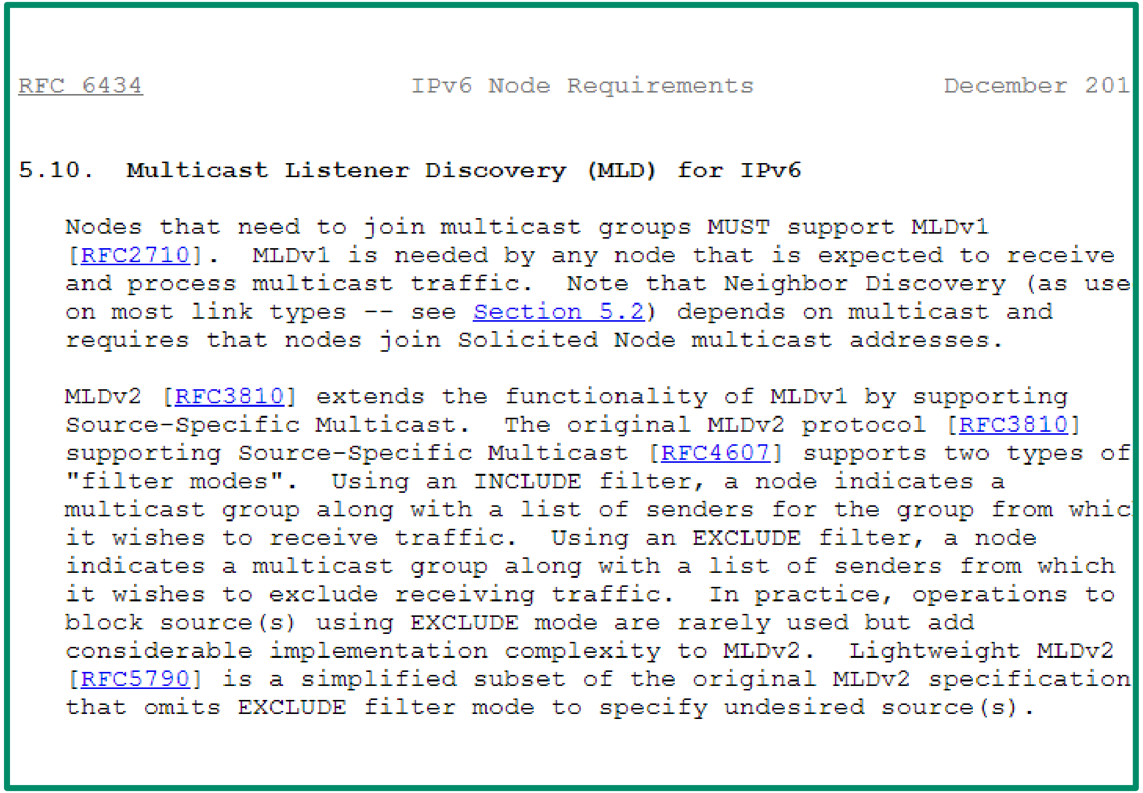
- Which, for bloated protocols at least, becomes increasingly difficult…

Complexity

More samples

- Extension Headers
- The rest of this slide intentionally left blank.
  - Ok, I couldn't refrain: again, Antonios is the man to ask about this lovely stuff.
  - Did (Fernando or) I already mention those are increasingly blocked anyway?
    - Please don't ask the obvious question why they're still around then.
    - Psst… don't google for "draft-filsfils"…





RFC 6434   IPv6 Node Requirements   December 201

5.10. Multicast Listener Discovery (MLD) for IPv6

Nodes that need to join multicast groups MUST support MLDv1 [RFC2710]. MLDv1 is needed by any node that is expected to receive and process multicast traffic. Note that Neighbor Discovery (as use on most link types -- see Section 5.2) depends on multicast and requires that nodes join Solicited Node multicast addresses.

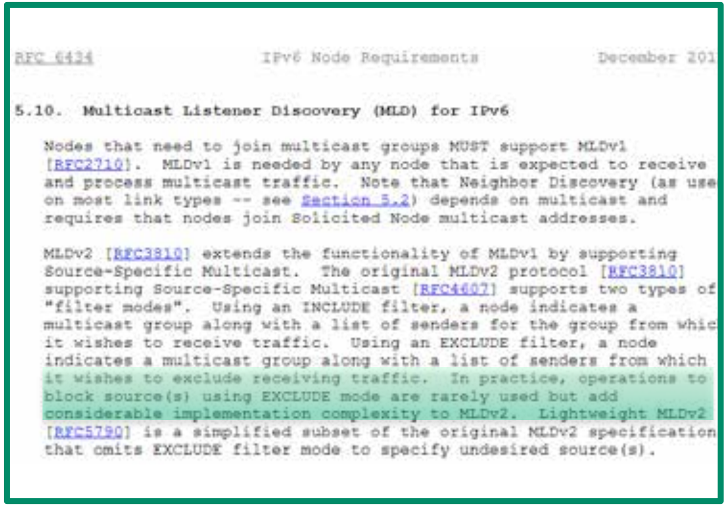
MLDv2 [RFC3810] extends the functionality of MLDv1 by supporting Source-Specific Multicast. The original MLDv2 protocol [RFC3810] supporting Source-Specific Multicast [RFC4607] supports two types of "filter modes". Using an INCLUDE filter, a node indicates a multicast group along with a list of senders for the group from whic it wishes to receive traffic. Using an EXCLUDE filter, a node indicates a multicast group along with a list of senders from which it wishes to exclude receiving traffic. In practice, operations to block source(s) using EXCLUDE mode are rarely used but add considerable implementation complexity to MLDv2. Lightweight MLDv2 [RFC5790] is a simplified subset of the original MLDv2 specification that omits EXCLUDE filter mode to specify undesired source(s).

Complexity

Here's another gem for you: MLD

MLD

In that short excerpt of RFC 6434 IPv6 *Node Requirements* on the previous slide…
did you notice?



```
RFC 6434                IPv6 Node Requirements              December 201

5.10.  Multicast Listener Discovery (MLD) for IPv6

   Nodes that need to join multicast groups MUST support MLDv1
   [RFC2710].  MLDv1 is needed by any node that is expected to receive
   and process multicast traffic.  Note that Neighbor Discovery (as use
   on most link types -- see Section 5.2) depends on multicast and
   requires that nodes join Solicited Node multicast addresses.

   MLDv2 [RFC3810] extends the functionality of MLDv1 by supporting
   Source-Specific Multicast.  The original MLDv2 protocol [RFC3810]
   supporting Source-Specific Multicast [RFC4607] supports two types of
   "filter modes".  Using an INCLUDE filter, a node indicates a
   multicast group along with a list of senders for the group from whic
   it wishes to receive traffic.  Using an EXCLUDE filter, a node
   indicates a multicast group along with a list of senders from which
   it wishes to exclude receiving traffic.  In practice, operations to
   block source(s) using EXCLUDE mode are rarely used but add
   considerable implementation complexity to MLDv2.  Lightweight MLDv2
   [RFC5790] is a simplified subset of the original MLDv2 specification
   that omits EXCLUDE filter mode to specify undesired source(s).
```

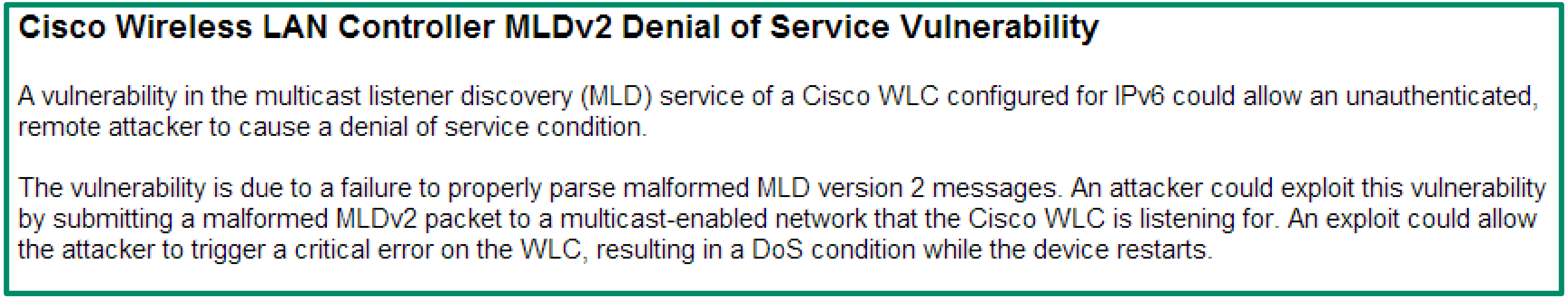
- There's four references to yet other RFCs.
- Apparently it tells us:

  "to work properly, ND – in itself simple & mature – needs MLD".

- MLD comes in different flavors (versions).
- I love this one:
  - "In practice, operations … are rarely used but add considerable implementation complexity"
  - IPv6 reality nicely summarized in one line!

Talking about MLD – 12 days ago

This is a classic:
“fail to properly parse”



Cisco Wireless LAN Controller MLDv2 Denial of Service Vulnerability

A vulnerability in the multicast listener discovery (MLD) service of a Cisco WLC configured for IPv6 could allow an unauthenticated, remote attacker to cause a denial of service condition.

The vulnerability is due to a failure to properly parse malformed MLD version 2 messages. An attacker could exploit this vulnerability by submitting a malformed MLDv2 packet to a multicast-enabled network that the Cisco WLC is listening for. An exploit could allow the attacker to trigger a critical error on the WLC, resulting in a DoS condition while the device restarts.

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140305-wlc

A Quick *Ceterum Censeo*

It helps to routinely re-read RFC 3439

Ceterum censeo
Carthaginem esse delendam.

Read 3439, sect. 5.3 on the *Simplicity Principle*.
Rinse & repeat.

RFC 3439, Again

The Coupling Principle states that as things get larger, they often exhibit increased interdependence between components.

- So, in IPv6, we have:
  - (Too many) Protocols
  - (Too many) Interactions
  - Extra spice (ext_headers et.al.)
- Have fun...

From Another Perspective

Some Wisdom from Economics

Elroy Dimson & Paul Marsh

“Calculating The Cost of Capital”

http://www.sciencedirect.com/science/article/pii/002463018290125X

Risk

- “More things can happen than will happen”
- I leave it up to you to reflect on this one, in the context of the last slides ;-)

What Else as for Properties

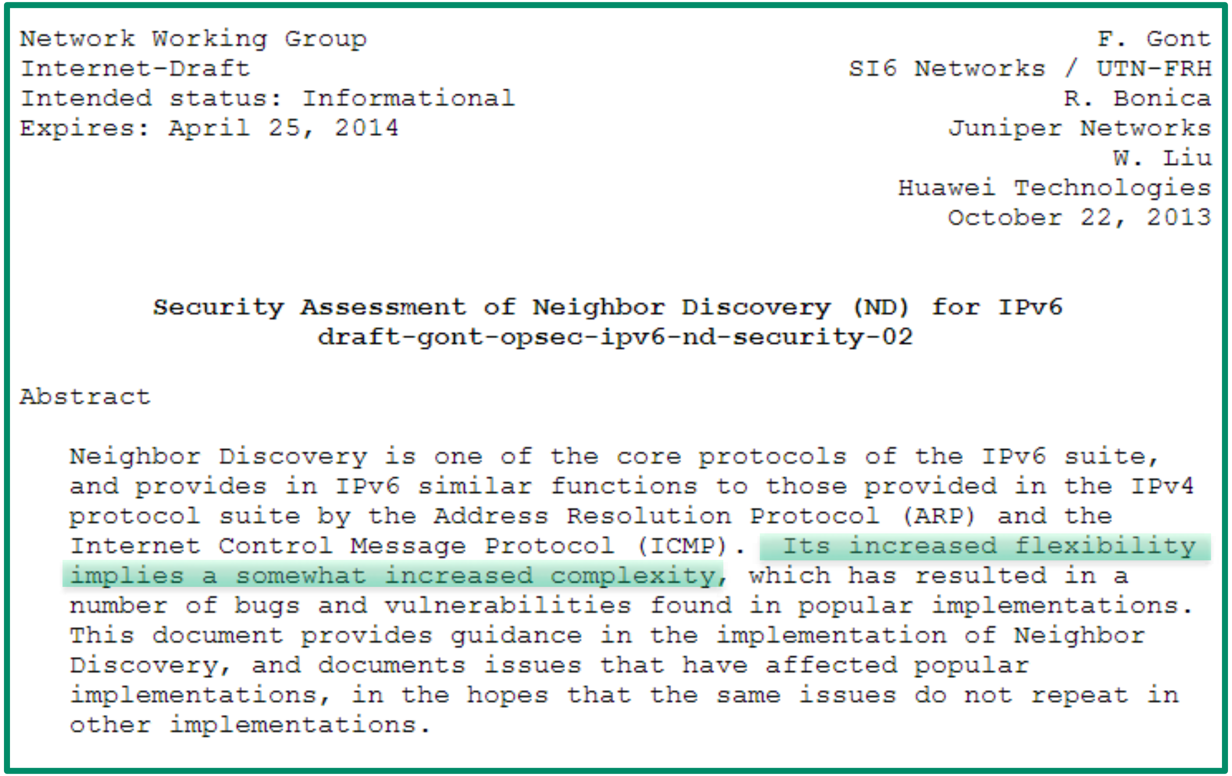
Two more important ones

- Trust Model

- "Integration of provisioning"

IPv6's Trust Model

On the *local link* we're all brothers.



```
Network Working Group                                            F. Gont
Internet-Draft                                     SI6 Networks / UTN-FRH
Intended status: Informational                                 R. Bonica
Expires: April 25, 2014                                 Juniper Networks
                                                                  W. Liu
                                                     Huawei Technologies
                                                        October 22, 2013


        Security Assessment of Neighbor Discovery (ND) for IPv6
                  draft-gont-opsec-ipv6-nd-security-02

Abstract

   Neighbor Discovery is one of the core protocols of the IPv6 suite,
   and provides in IPv6 similar functions to those provided in the IPv4
   protocol suite by the Address Resolution Protocol (ARP) and the
   Internet Control Message Protocol (ICMP).  Its increased flexibility
   implies a somewhat increased complexity, which has resulted in a
   number of bugs and vulnerabilities found in popular implementations.
   This document provides guidance in the implementation of Neighbor
   Discovery, and documents issues that have affected popular
   implementations, in the hopes that the same issues do not repeat in
   other implementations.
```

We're All Brothers

I like the idea. Really.

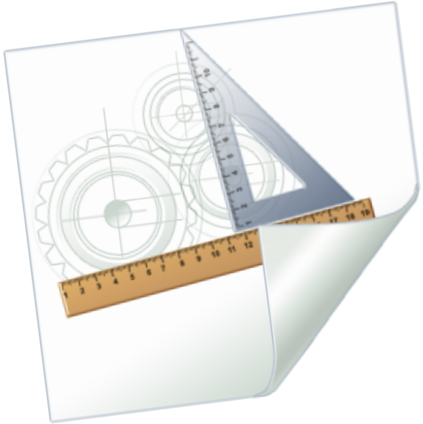
As much as I like the concept of eternal happiness & peace.

What's a *Router*?

- Wikipedia:
  - router = "a **router** is a device that forwards *data packets* between *computer networks*"
- RFC 2460:
  - router: "router - a node that forwards IPv6 packets not explicitly addressed to itself."
- Is there any issue then?

What's a *Router,* in IPv6?

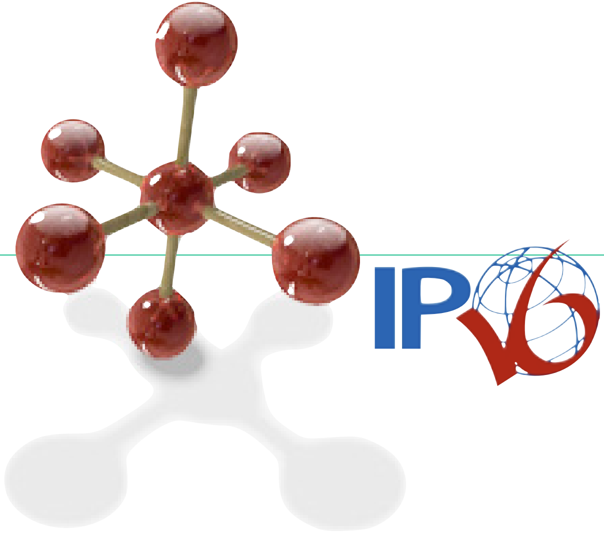
Looking Closer



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

- In the end of the day, in IPv6 a router is not just a forwarding device but a provisioning system as well.
  - As many other IPv6 guys I generally like the idea.
  - Still, having an operations background in large scale enterprise networks I can tell you quite some of my colleagues have a hard time with this.
  - While we're at it: MANY THANKS TO YOU GUYS OVER THERE AT IETF FOR THE BRILLIANT STATE OF RA & DHCPv6 "INTERACTION".
    - This really helps a lot with widespread IPv6 adoption. Rly!
  - That said I won't further open this can of worms here…

Impact



Enough Ranting on Standards & Specs

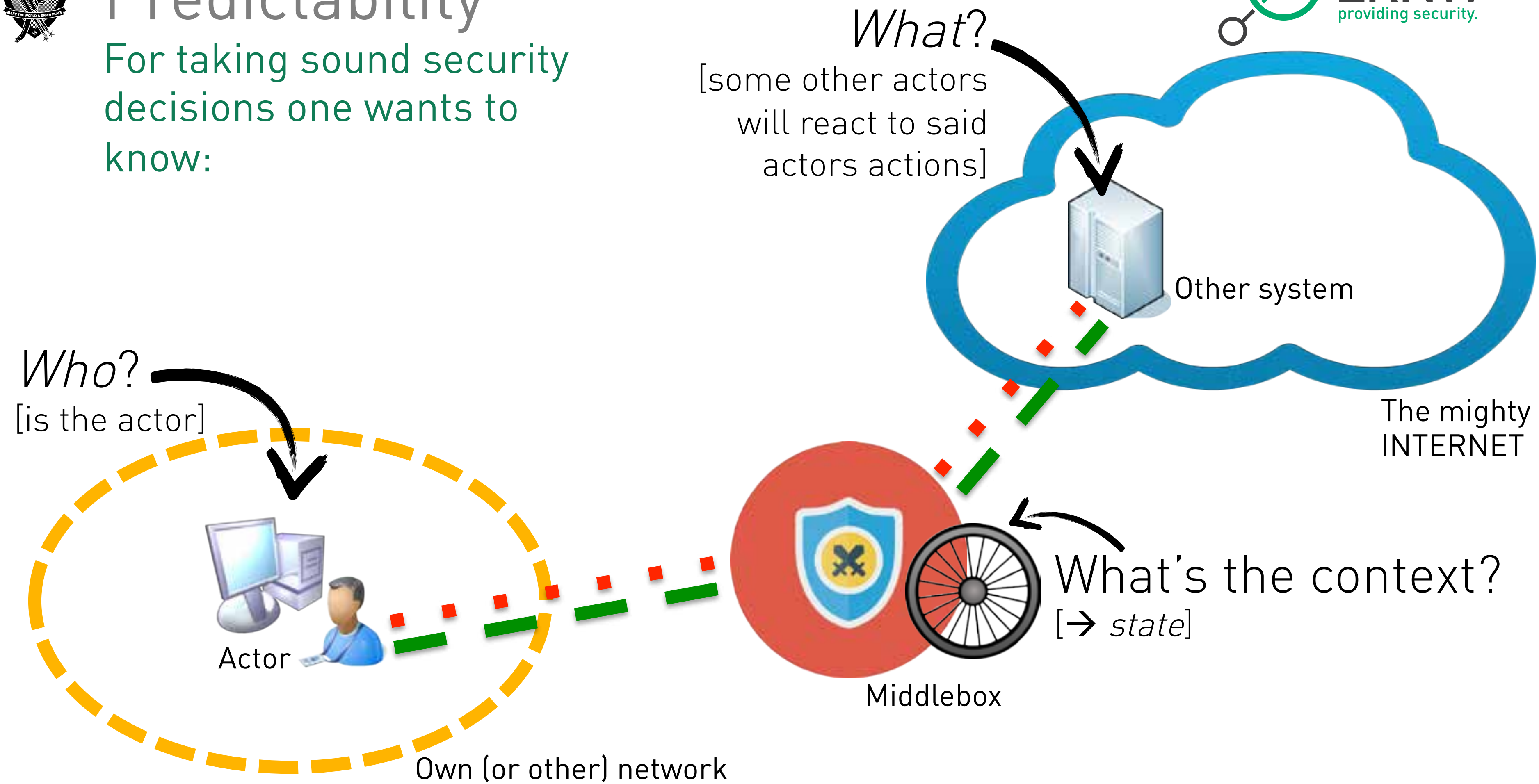
Taking an infosec practitioner's view:

What are typical elements of current security models?

- Predictability
  - RFC 2828: "trust: the extent to which someone who relies on a system can have confidence that the system meets its specifications, i.e., that the system does what it claims to do and does not perform unwanted functions"
- Identification
  - Be able to identify actors (for security enforcement or audit).
- Classification
  - Gather sufficient information to take well-informed decisions.
- Capabilities
  - To enhance/assure identification & classification information.
  - To enforce security policy.
- (Retention of) State
  - As a supporting tool for classification & enforcement.
- Simplicity
  - What? ;-)

Predictability

For taking sound security decisions one wants to know:



What?

[some other actors will react to said actors actions]

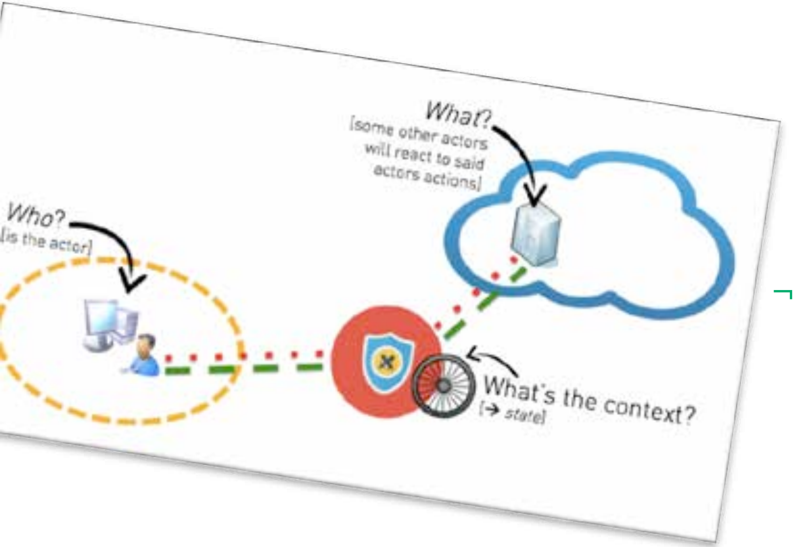
Who?

[is the actor]

What's the context?

[→ *state*]

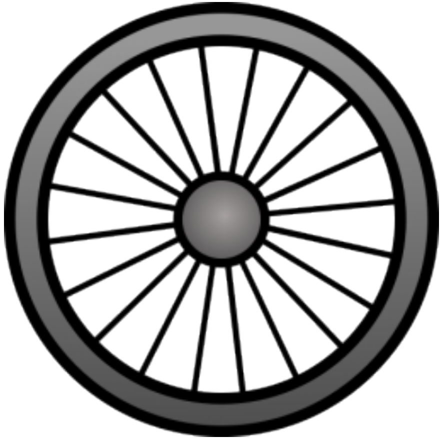
In IPv6 All These Might Be Hard



- Who?
  - Privacy Extensions being the norm now.
  - Yes, identifying an actor (client machine) by its IP address can be done (Eric will discuss this in the afternoon), it's just operationally much harder.

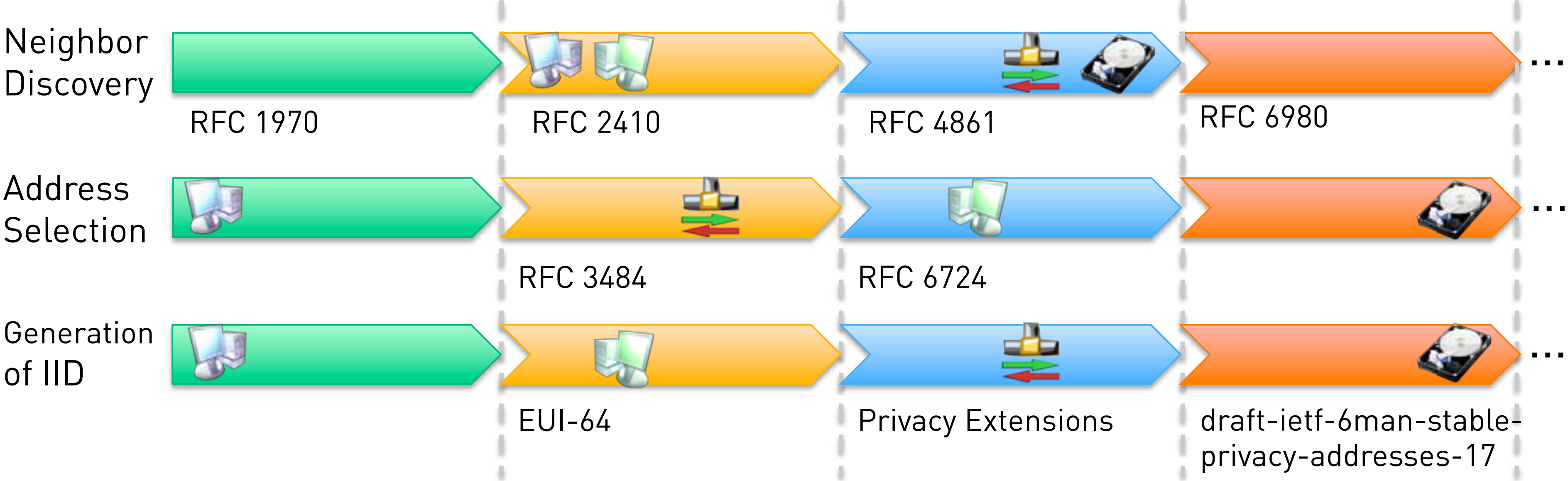
    And there's a direct relationship between *operational feasibility* and real-life security. You all knew that, of course.
- What?
  - Not one stack behaves like another one.
  - Not one firewall behaves like another one.
  - Not one network device behaves like another one.
  - Etc.
- State
  - Might be very difficult to keep.

State



- In the end of the day, *neighbor cache exhaustion (NCE)* is a *state* problem
  - ARP had an *incomplete* state as well.
  - You just rarely saw segments > 24 exposed to the Internet. At least in (most) enterprises. I'm well aware of you guys running academic networks ;-)
- Let's assume NCE is a mostly solved problem.
  - Btw: by vendor-specific tweaks which might not be documented very well. ⇔ predictability, once again.
- Still, there's much more opportunities for a state oriented sec model to fail in the IPv6 age
  - I'm very interested to see how vendors of stateful firewalls will handle scenarios like "single infected machine sitting in a broadband /64 and establishing valid connections to web server from many many random source addresses". BCP 38 won't solve this.

Back to that IPv6'n'RFCs Time Bar ...



Neighbor Discovery

RFC 1970

RFC 2410

RFC 4861

RFC 6980

...

Address Selection

RFC 3484

RFC 6724

...

Generation of IID

EUI-64

Privacy Extensions

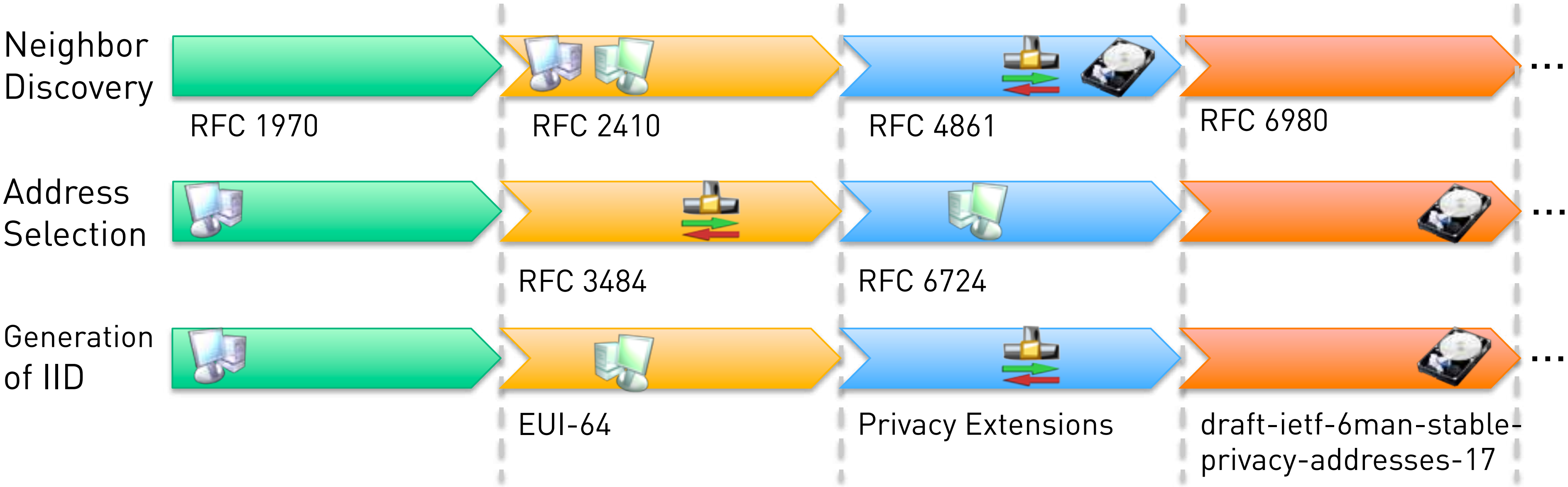
draft-ietf-6man-stable-privacy-addresses-17

...

NOW:

- ✓ Please spot ... for $OS in your environment.
- ✓ Please spot ... for $OTHER_OS in your environment.
- ✓ Please spot ... $EACH_TYPE_OF_NETWORK_DEVICE
- ✓ Please spot ... $STORAGE_DEVICES

Introducing the magic IPv6'n'RFCs time bar ;-)



NOW:

- ✓ Please spot … for $OS in your environment.
- ✓ Please spot … $STORAGE_DEVICE

#GOtoFAIL ☹

Capabilities

Just a short note

- You do not really expect your current set of middlebox hardware & software to *fully* support IPv6, do you?

- Christopher's & Antonios' workshop tomorrow might provide orientation…

What does all this mean for us?

Avoid (Additional) Complexity at All Costs!

- You have enough of that anyway.
- Keep your addressing scheme as simple & clean as possible.
  - For most of your environments & use cases this includes: go with GUAs only.
- Wherever possible avoid *deviation from default.*
  - https://www.ernw.de/download/ERNW_ACSAC_IPv6_High_Secure_Networks.pdf
- Whenever you think of enabling a device's (IPv6/sec) feature or some host based parameter, re-read RFC 3439.

What All This Means for You (II)

"Some things in life can never be fully appreciated nor understood unless experienced firsthand. Some things in networking can never be fully understood by someone who neither builds commercial networking equipment nor runs an operational network."

RFC1925, 2.4

- IPv6 is not a paper exercise
  - In environments where stability & security are relevant – and why else would you be listening right now ;-) – you MUST test, test, test!
  - Yes, I know, mgmt doesn't like that extra budget for an "IPv6 test lab"…

For good cause.

Do Not Place Too Much Security Burden on State

Middlebox:

"any intermediary box performing functions apart from normal, standard functions of an IP router on the data path between a source host and destination host."

RFC 3234

- You might not be able to maintain sufficient state on middleboxes in IPv6 networks.
  - → Re-engineer security models
  - Stateless ACLs, isolation and so on

Conclusions

- The IPv6 protocol space is a huge mess, full of complexity.
  - Please don't shoot the messenger (me).
  - Dear IETF: it gets worse every day.
- You (audience) still have to deal with the situation
  - Do your homework. Read specs & get your hands dirty (testing).
- You might not show this presentation to your CIOs ;-)

This is my final statement.

Thanks for listening!

Enjoy #IPv6SecSummit & #TROOPERS14!

> "RFC 1925. sect 12:
> In protocol design, perfection has been reached not when there is nothing left to add, but when there is nothing left to take away."

https://tools.ietf.org/html/rfc1925