Abuse of CPE Devices and Recommended Fixes

Dr. Paul Vixie (Farsight Security, Inc.)
Chris Hallenbeck (US-CERT, DHS)
Jonathan Spring (CERT/CC, Carnegie Mellon)

August 7, 2014
Black Hat USA 2014

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution.

DM-0001511

Based on a CERT whitepaper

“Abuse of Customer Premise Equipment and Recommended Actions”

Goals:

1. Make sure everyone is on the same page
2. Measure what we’ve all assumed
3. What we need to do about the problem

What is CPE?

“Customer Premise Equipment”

Home router

PBX

Phones

i.e. what interfaces with the telco provider

(Photo: Jörg Kantel, CC 2.0 license)

PBX image source: Wikipedia user Adamantios

Threats that abuse CPE (I)

The home router is a network proxy for most things on your home network

So own that and you control even well-defended devices on the home network

DNS changer botnet

- Attempted to reconfigure home router DNS server to only use adversary's DNS server
- See FBI's "Operation Ghost Click"

Threats that abuse CPE (II)

DDoS – DNS reflection and amplification

- Home routers run a recursive DNS server
- If it is misconfigured to be “open”
  - Anyone can ask it anything
- Spoof UDP packets with target in source IP

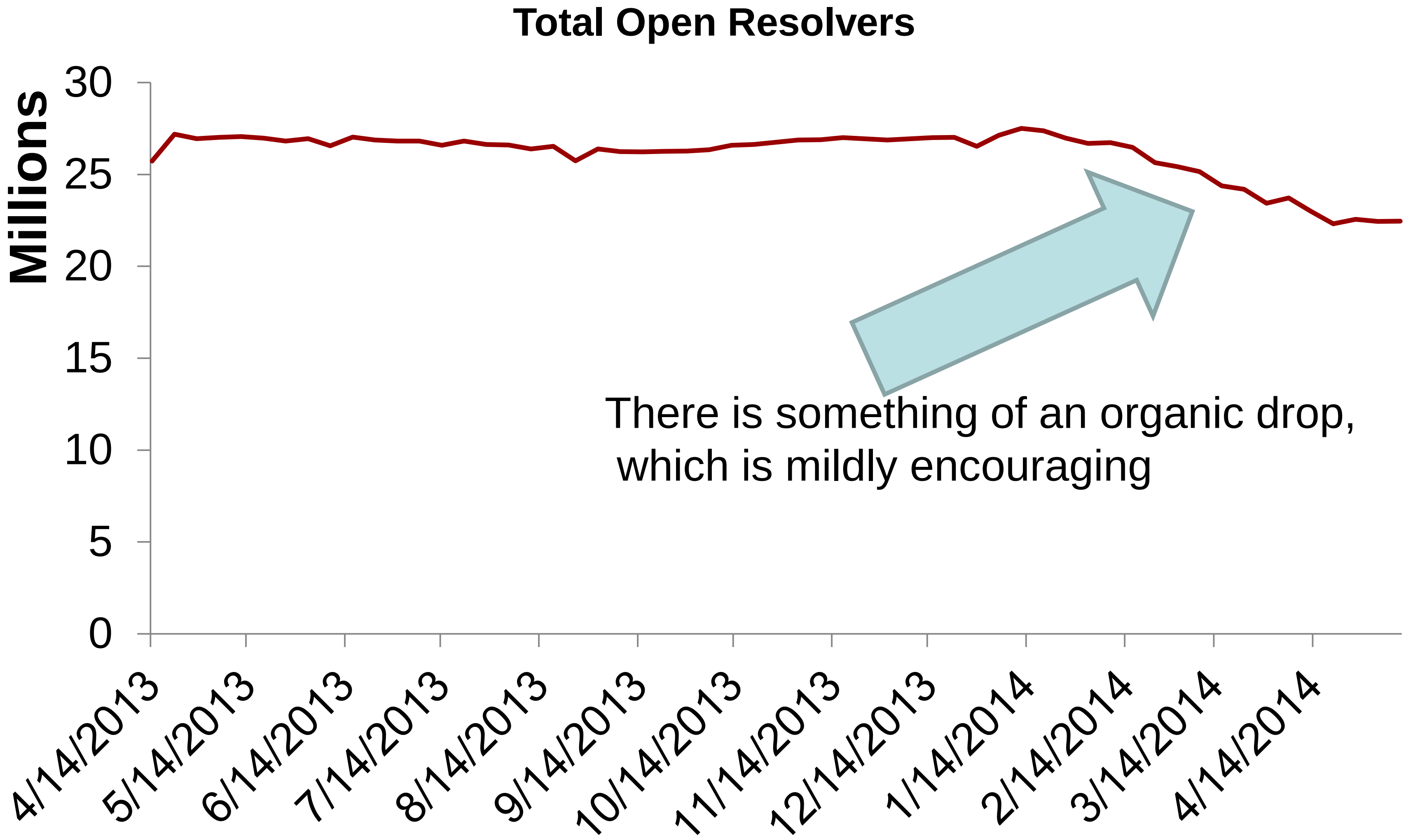
Reflection

- Anonymizes attacker, makes hard to block

Amplification

- Responses are 20 times larger than requests
- (up to 50 times if DNSSEC is used)

How many open resolvers?



There is something of an organic drop, which is mildly encouraging

Data source: OpenResolverProject

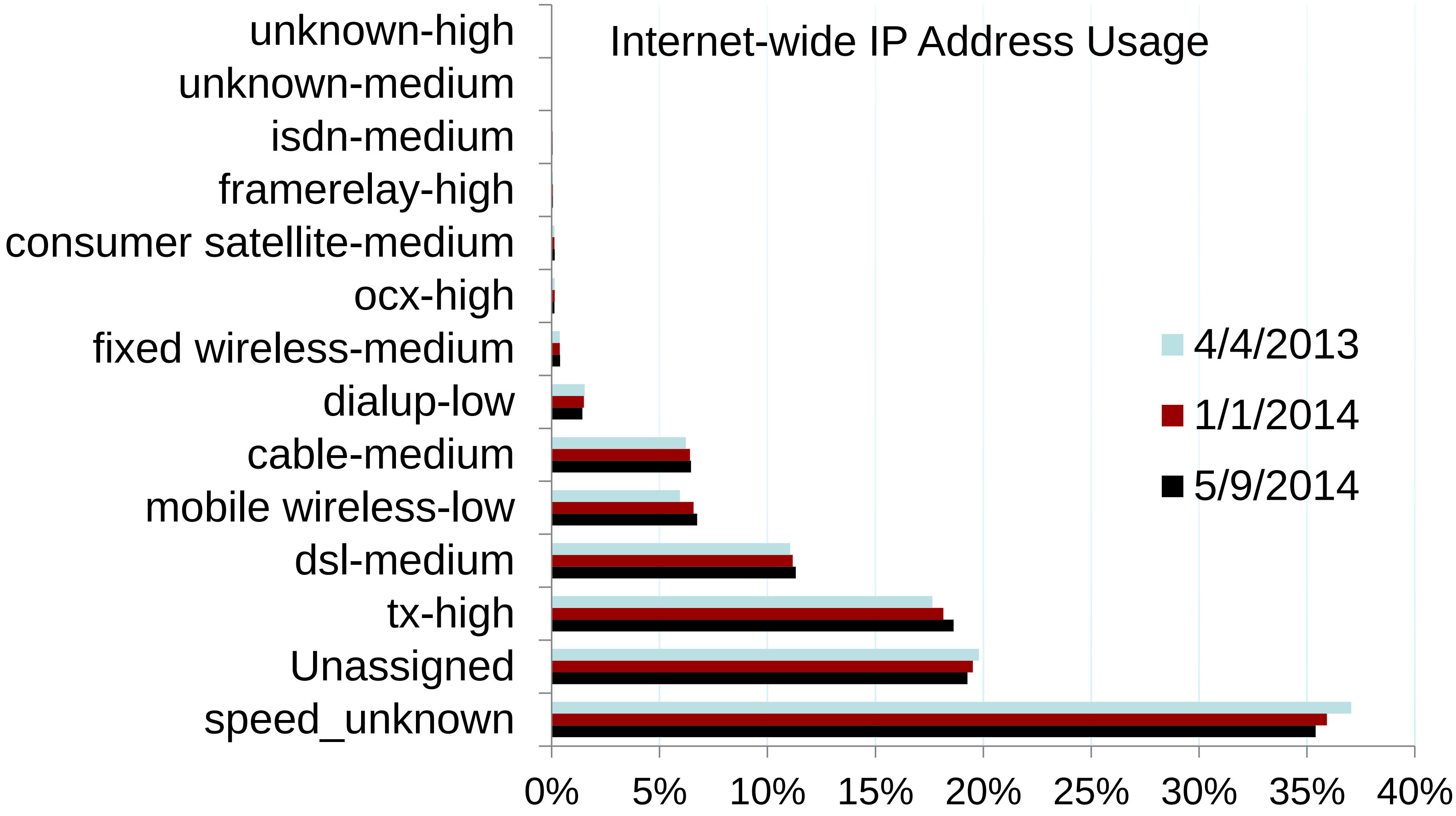
Where are they?

It’s hard to say exactly what device is the open resolver.

But the link speed of the connection gives a good clue as to if it is a home or small-business user as compared to an enterprise

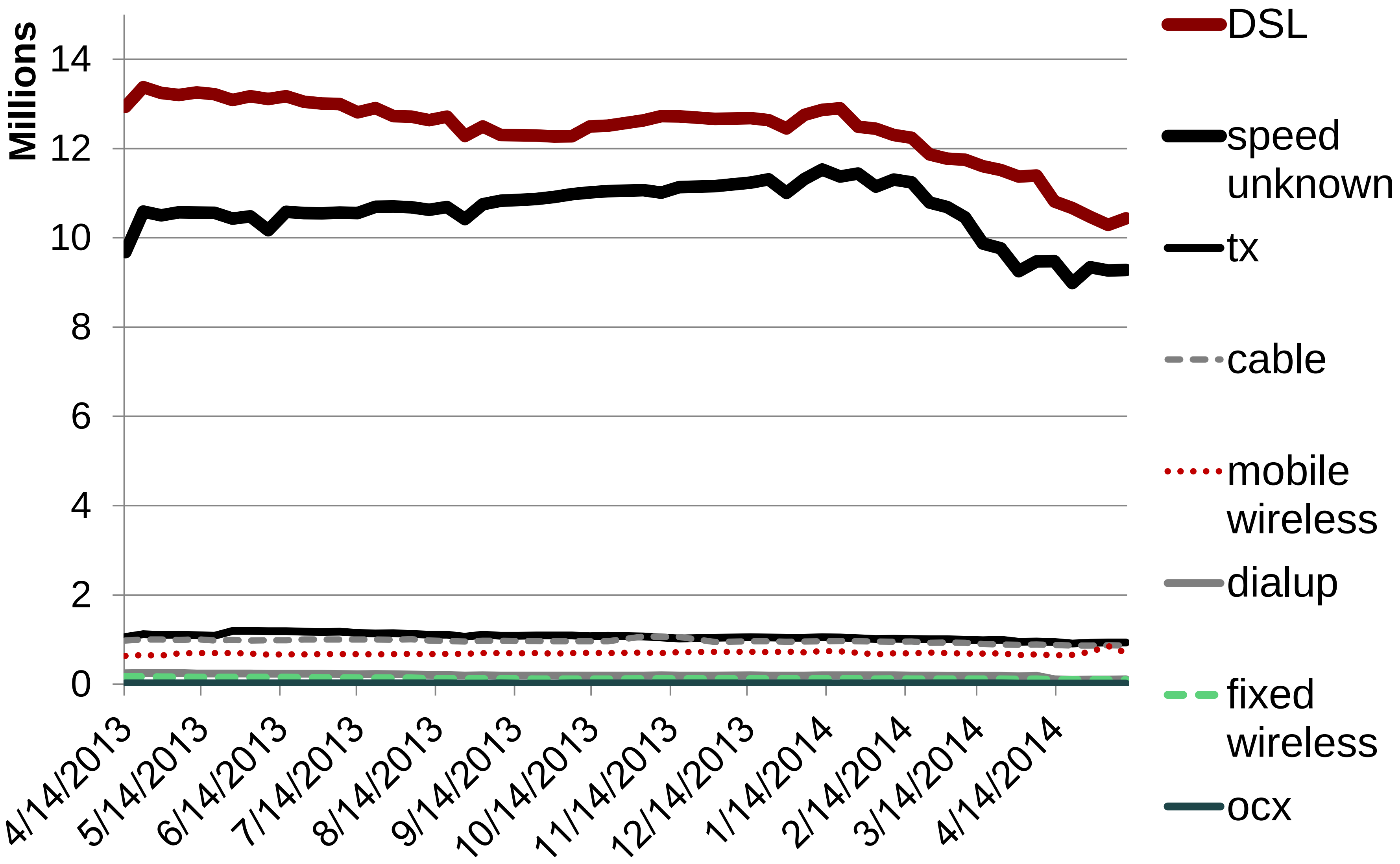
- Enterprises usually lease lines, or are high-speed
- Small users tend to be on DSL, cable, etc.

Where are they? – Internet connection and speed baseline



Connection type and speed data source: Neustar

Where are they? – Open resolver link speed



Where are they?

They’re on DSL links

- 11% of the Internet
- 50% of open resolvers

They’re not on enterprise links

Thus it seems the open resolver issue is disproportionately a CPE issue.

What do we do?

Device manufacturers need a path for continuous upgrades

Implement source address validation

Reconfigure each device so it can't be leveraged quite so effectively

Responsibility to manufacturers and providers

Continuous upgrades

Current regime is fire-and-forget

There is little to no user interface

Updates, such as they are, are very manual

Home routers may not be replaced until they break

- They’re not shiny or forced into obsolescence like phones

There’s no path for continuous upgrades

- And there are plenty of vulnerabilities to exploit[1]

[1] CVE-2014-0356, CVE-2014-0354, CVE-2014-0353, CVE-2014-1982, CVE-2014-2925, CVE-2014-3792, CVE-2013-4772, CVE-2014-2719, CVE-2013-5948, CVE-2014-0337, CVE-2014-1599, CVE-2013-3365, CVE-2013-3098, CVE-2014-0329, CVE-2013-3090, CVE-2013-3087, CVE-2013-3084, CVE-2013-6343, CVE-2014-0659, CVE-2013-7282, CVE-2013-7043, CVE-2013-6918, CVE-2013-3095, CVE-2013-2271, CVE-2013-5703, CVE-2013-6027, CVE-2013-6026

Source address validation

Prevent forged packets from being sent in the first place

http://tools.ietf.org/html/bcp38 (also BCP 84)

www.icann.org/en/committees/security/sac004.txt

This has been well documented for a while now

No seriously, please.

@ customer-facing edge

@ data centers

Responsibility

Who is responsible for the data emitted or forwarded as the result of misconfigurations and errors?

- Manufacturers
- Providers who manage configs

The incentives must be arranged so that those responsible can and will fix the issues.

Responsibility – proper incentives

Short-term individual costs are trumping long-term community gains

- This is predicted by game theory.
- Well, predicted for irrational agents under certain conditions

These public Internet health risks are treated as externalities and “not my problem”

These risks need to be internalized and shared evenly somehow

CERT

Thanks for Listening!

Questions?
Comments?