

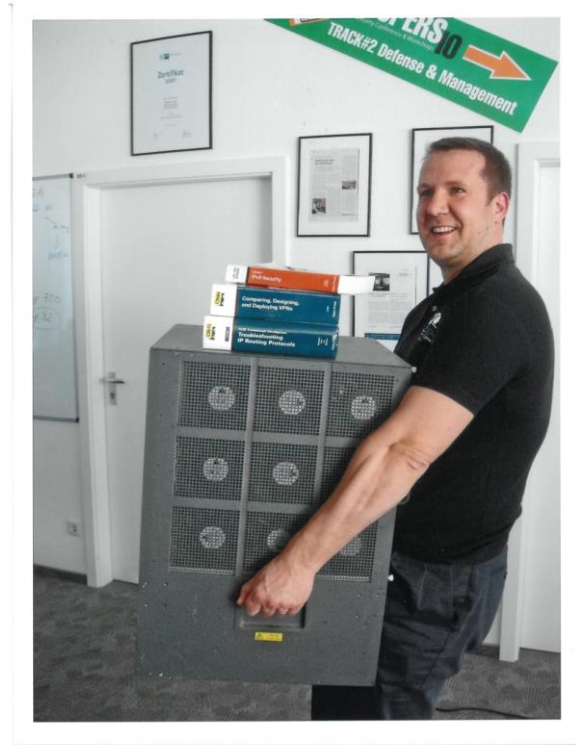


Balanced Security for IPv6 CPE Revisited

Enno Rey, erey@ernw.de
[@Enno_Insinuator](https://twitter.com/Enno_Insinuator)

#whoami

- Networking background, doing security as a full-time profession since 1997
- Taking care of LIR stuff at some enterprise LIRs
 - Including the one with this nice handle:
ORG-HACK1-RIPE
- Blogging about IPv6 & other pieces at <https://insinator.net/tag/ipv6/>



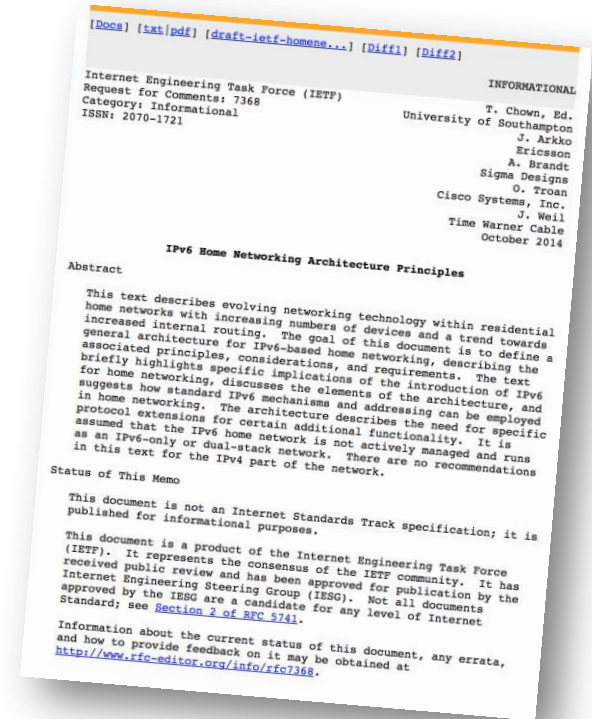
Agenda

- Implications of IPv6 for “Home Networks”
- Actors in the Ecosystem and Their Responsibilities
- Conclusions & Proposals



Home Networks

- I loosely follow definition/concept laid out in RFC 7368
 - C[P]E separating homenet from provider's network.
- Those networks being connected/separated by “residential Internet gateways” as of RFC 6092 definition.



Some Wisdom from RFC 6092

The reader is cautioned always to remember that the typical residential or small-office network administrator has no expertise whatsoever in Internet engineering. Configuration interfaces for router/gateway appliances marketed toward them should be easy to understand and even easier to ignore. In particular, extra care should be used in the design of baseline operating modes for unconfigured devices, since most devices will never be changed from their factory configurations.

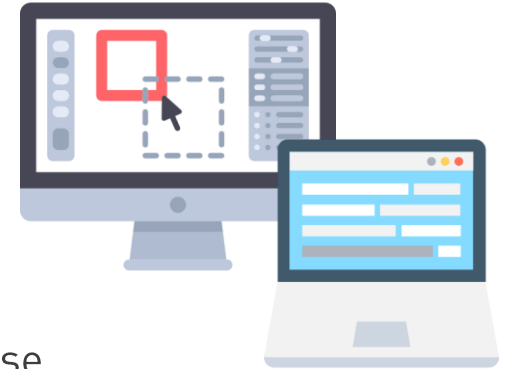
Types of Devices to be Seen in Home Networks

- Desktop & laptop computer systems
 - Usually some interaction with a human user here.
 - Most have an OS with auto-update mechanism.
 - In general they don't come with services like Telnet or HTTP enabled by default AND weak credentials on those.



Types of Devices to be Seen in Home Networks

- Desktop & laptop computer systems
 - Usually some interaction with a human user here.
 - Most have an OS with auto-update mechanism.
 - In general they don't come with services like Telnet or HTTP enabled by default AND weak credentials on those.
- IoT Devices
 - Let's just go through the above list...



Stephen A. Ridley
@s7ephen

Following

If you're new to vuln research, and you lament that "real bugs" are too hard to exploit in "modern" OSes, you need to be looking at [#IoT](#)

7:03 PM - 26 Aug 2017

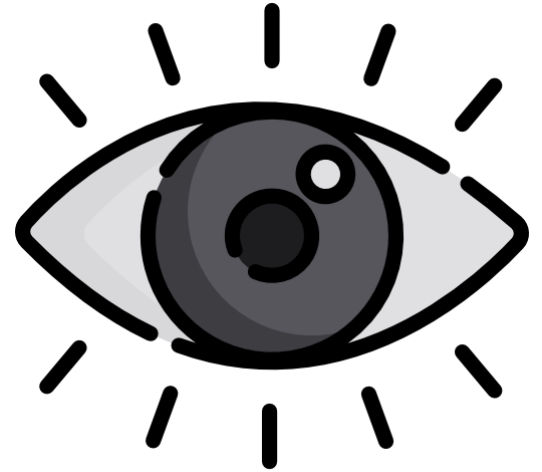
IoT Devices in the Home – Some more Notable Differences

- Inhabitants might not even know they're there.
- Lifetime, in general, plus its relationship with
 - Availability of updates/patches
 - Liability/warranty (if any)
 - Strength of crypto (but probably least of problems)
- Potential interaction with physical world.



Implications of IPv6 for Home Networks

- Fully globally routable address space used for devices
- Some people think that this will not necessarily lead to “global visibility”
 - Large address space (/64), combined with
 - Random addresses as of RFCs 4941 or 7217.
- Some people disagree on the above
 - Malware might use “smart scanning” (see RFC 7707)
 - Shodan abuse of ntp.org pools
 - <http://seclists.org/oss-sec/2016/q1/219>



Implications on User Expectations & Trust

- Even if we agreed that the restoration of E2E on the Internet is a desirable technical goal ...
- There's (the vast majority) of non-technical users, with their own perceptions & expectations.
- Hypothesis: the stateful nature of NAT44 and its inherent impact on inbound connectivity has led to a certain mental image.



This Is What (I Think) Many Users Believe





While This Is Reality



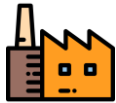



Actors in the Ecosystem & Their Responsibilities Incentives

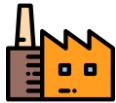


Actors in the Ecosystem & Their Responsibilities Incentives

- Vendors (of devices) 





Actors in the Ecosystem & Their Responsibilities Incentives

- Vendors (of devices) 
- Providers “bringing Internet to the home” 

Actors in the Ecosystem & Their Responsibilities Incentives

- Vendors (of devices) 
- Providers “bringing Internet to the home” 
- Users 

Actors in the Ecosystem & Their Responsibilities Incentives

- Vendors (of devices) 
- Providers “bringing Internet to the home” 
- Users 
- Several types of 3rd parties, providing value-add services of all types 



... And Their Incentives

... And Their Incentives

- Vendors
 - Be quick (to market), cheap and easy-to-use



... And Their Incentives

- Vendors
 - Be quick (to market), cheap and easy-to-use



- Users
 - Whatever.



... And Their Incentives

- Vendors
 - Be quick (to market), cheap and easy-to-use



- Users
 - Whatever.



- 3rd Parties
 - Be (minimum) compliant, make money



... And Their Incentives

- Vendors
 - Be quick (to market), cheap and easy-to-use



- Users
 - Whatever.



- 3rd Parties
 - Be (minimum) compliant, make money



- Providers



Crucial Question

- Do we (Providers) have an ethical obligation to protect users?
 - If so in which way?



Crucial Question

- Do we (Providers) have an ethical obligation to protect users?
 - If so in which way?

- If not, what could be (financial) reasons to do so?



Crucial Question

- Do we (Providers) have an ethical obligation to protect users?
 - If so in which way?
- If not, what could be (financial) reasons to do so?
 - Less customer service calls?



Crucial Question

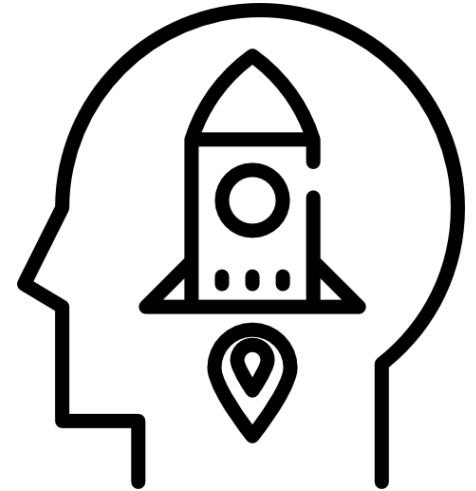
- Do we (Providers) have an ethical obligation to protect users?
 - If so in which way?
- If not, what could be (financial) reasons to do so?
 - Less customer service calls?
 - Minimize collateral damage from large-scale DoS?
 - Tragedy of commons. See history of BCP38...



Here's an Opinion

- Yes, we (RIPE community) do have such an ethical obligation.
 - If we don't do it, who else?
 - We have the technical means & skills.
 - In today's Internet we can't plead a "mere conduit" stance.

- I'm happy to incite a lively debate (not only) right after this talk ;-)



Where Providers Can Influence/Have an Impact


- Security-related (default) configuration of CPE







Filtering on the CPE – Approaches




Filtering on the CPE – Approaches

- Do nothing (→ no filtering at all) 

Filtering on the CPE – Approaches

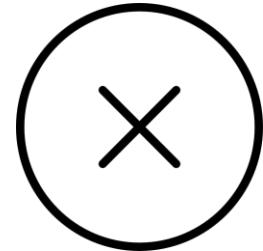
- Do nothing (→ no filtering at all) 
- Filter pretty much all inbound connections 

Filtering on the CPE – Approaches

- Do nothing (→ no filtering at all) 
- Filter pretty much all inbound connections 
- Something in between 

Approaches (I): No Filtering at All

- To the best of my knowledge a few do this
 - Apparently Fortinet (GR) amongst them.
- On technical mailing lists usually there are some people who like this approach
 - *They* have experience & expertise to evaluate risks and to secure stuff behind CPE.



Approaches (II): Block “Unsolicited Inbound”

- (Informational) RFC 6092 *Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service*
 - Block inbound stuff (which doesn't have state) except some ICMPv6 and IPsec.
- There are several variants & flavors of this (e.g. include IPsec in blocked stuff).
- From my perspective quite some providers (the majority?) somewhat follow these lines.



Approaches (III): “Balanced Security”

- Allow most inbound traffic, but filter “known bad” stuff
 - Evidently this requires some weighting & trade-offs, plus constant re-evaluation.
- Draft Balanced Security for IPv6 Residential CPE.
draft-ietf-v6ops-balanced-ipv6-security
 - Withdrawn in IETF v6ops in mid 2014, at rev 01.
 - Main discussion
 - <http://lists.cluonet.de/pipermail/ipv6-ops/2012-November/007934.html>



Balanced IPv6 Security

Transport	Port	Description
tcp	22	Secure Shell (SSH)
tcp	23	Telnet
tcp	80	HTTP
tcp	3389	Microsoft Remote Desktop Protocol
tcp	5900	VNC remote desktop protocol

Table 1: Drop Inbound

Statements on v6ops ML (I)

- “These days, people lug around their computing devices all the time, connecting them indiscriminately to various public wireless networks”
 - Does not apply to IoT devices @ home.
- “The operating systems that were notorious for being vulnerable to worms and other traffic from the internet, simply do not support IPv6.”
 - Might have been true 5 years ago. I’m not so sure as for the future...
- “The majority of attacks these days come through other channels than direct inbound connections.”
 - Really? What about Mirai?
And IoT devices do not click on links in e-mails...



Statements on v6ops ML (II)

- “By doing firewalling as a default service, you are implicitly taking on responsibility”
 - Yes, exactly! That’s what this is about, somewhat... [however not in legal/liability sense anyway]
- “Sticking them on an internet link with no line of defence between them and their attackers seems like a really bad idea to me.”
 - That’s what I think, too.



How Could a Potential Contribution Look Like?

- Collection of data points
 - We (ERNW) have started a small research project analysing the actual posture of several providers (mainly) in Germany.
- Start a BCOP document?
 - I'd be willing to write a draft and present (on) it at RIPE76 (Marseille).



There's never enough time...

THANK YOU...

...for yours!



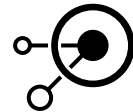
@Enno_Insinuator



erey@ernw.de



ernw.de



insinuator.net



Slides available soon.

The Looming Threat of Regulation – To Keep in Mind?

- Will it happen (anyway)?
 - If so which parties will be affected?
- See also
 - “Proposed US legislation” discussion on [iot-discussion] in Aug 2017



Sources

Image Source:

- Icons made by [Freepik](http://www.flaticon.com) from www.flaticon.com

