University of Glasgow

Internet Protocols Laboratory

RIPEn at Home

Surveying Internal Domain Names using RIPE Atlas

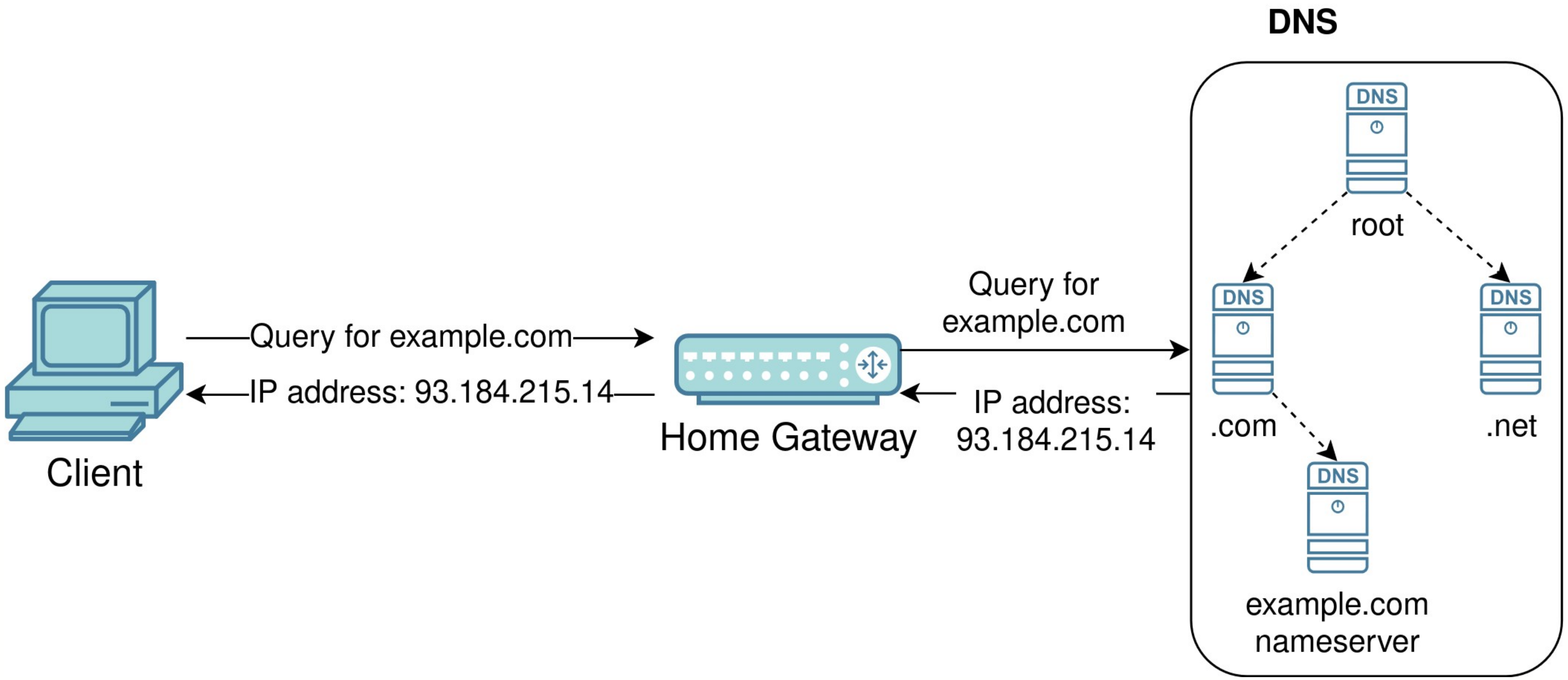
Elizabeth Boswell (e.boswell.2@research.gla.ac.uk)
Colin Perkins

Introduction

- What is the Domain Name System?
- What are internal names?
- Name collisions and FRITZ!Box case study

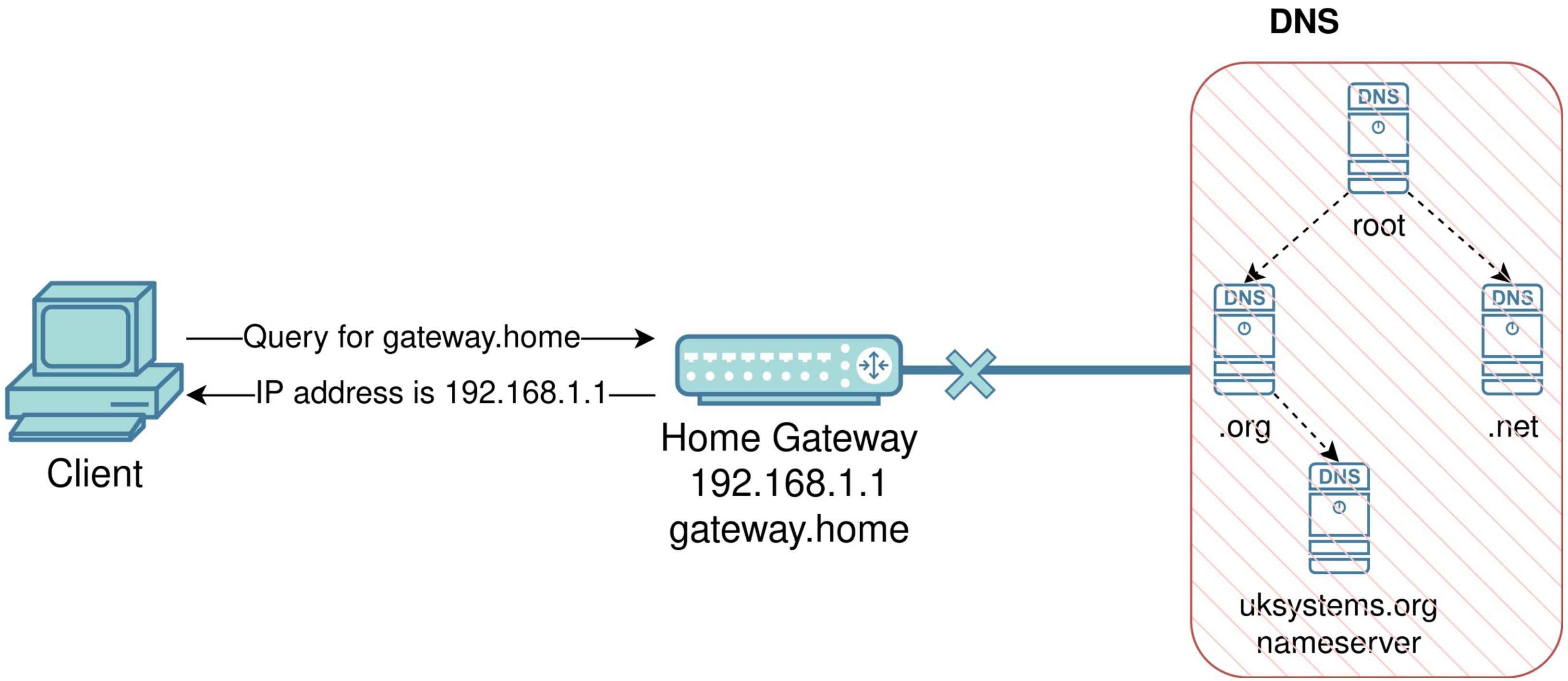
The Domain Name System (DNS)

- Maps domain names (e.g. example.com) to other data (mainly IP addresses)
- Hierarchical system with a single root
- **Top-level domain (TLD):** rightmost label (e.g. com)



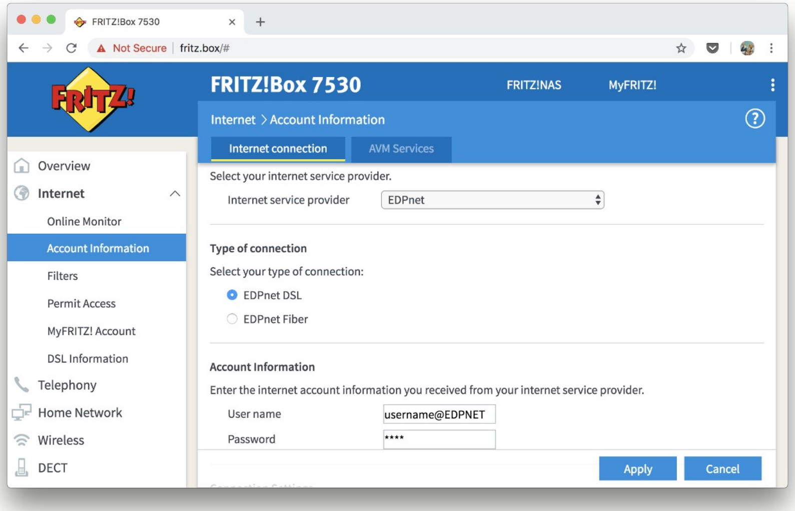
Internal Names and Name Collisions

- **Internal names:** Domain names that are only valid in the local network
  - Queries shouldn't be sent to the global DNS
- **Name collision:** query for internal name is sent to the DNS, response differs



Case Study: FRITZ!Box vs .box

- AVM FRITZ!Box: popular home gateway in Europe
- When connected to FRITZ!Box, can access the configuration page at fritz.box
- .box top-level domain (TLD) now in the DNS, advertised to the public in January 2024
- Web3 project – many names bought speculatively
- fritz.box and related domains were owned by speculators for several weeks



Select your internet service provider.

Internet service provider: EDPnet

Type of connection

Select your type of connection:

● EDPnet DSL

○ EDPnet Fiber

Account Information

Enter the internet account information you received from your internet service provider.

User name: username@EDPNET

Password: ****

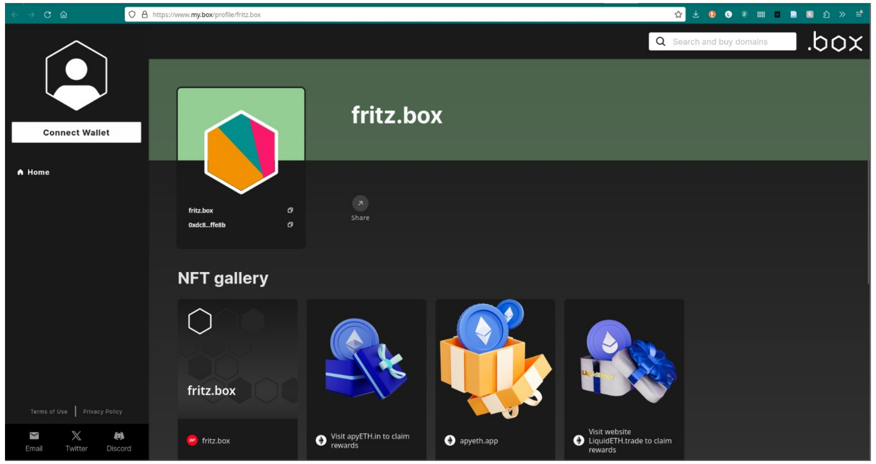

https://www.my.box/profile/fritz.box
Search and buy domains
.box
Connect Wallet
Home
fritz.box
fritz.box
0xdc8...ffe8b
Share
NFT gallery
fritz.box
fritz.box
Visit apyETH.in to claim rewards
apyeth.app
Visit website LiquidETH.trade to claim rewards
Terms of Use | Privacy Policy
Email
Twitter
Discord

Image sources: https://www.edpnet.be/en/support/installation-and-usage/internet/manage-fritz!box/how-do-i-install-and-configure-my-fritz!box-7530.html and https://my.box/profile/fritz.box (identical to fritz.box at the time)

fritz.box Collision

- fritz.box name **resolves differently** depending on whether the query goes to a FRITZ!Box gateway or the public DNS
- Queries can **inadvertently be sent** to the public DNS, e.g. when using a public resolver or when connected to a different network
- **Security risk:** the “public” fritz.box could **spoof** the FRITZ!Box

Surveying Internal Names

- Research aims
- Internal name detection methodology
- Results
- Next steps

Surveying Internal Domain Names

- Which internal domain names are **used by home gateways**?
- Which of these are currently **at risk of name collision**?
- Which **would be at risk of name collision** if their top level domain (TLD) was added to the DNS?

RIPE Atlas

- Globally distributed measurement network
- ~10,000 probes (small computers or virtual machines) in various networks, including home networks
- Probes are vantage points for network measurements, including traceroute and DNS queries

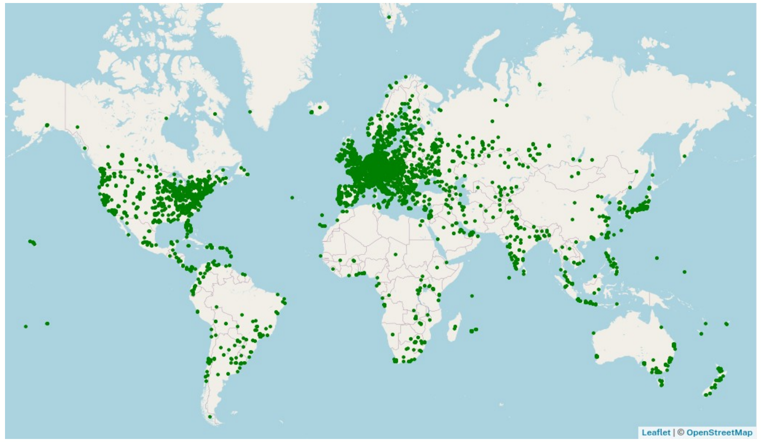


Image sources: https://labs.ripe.net/author/alun_davies/new-ripe-atlas-version-4-probes/ and https://atlas.ripe.net/coverage/

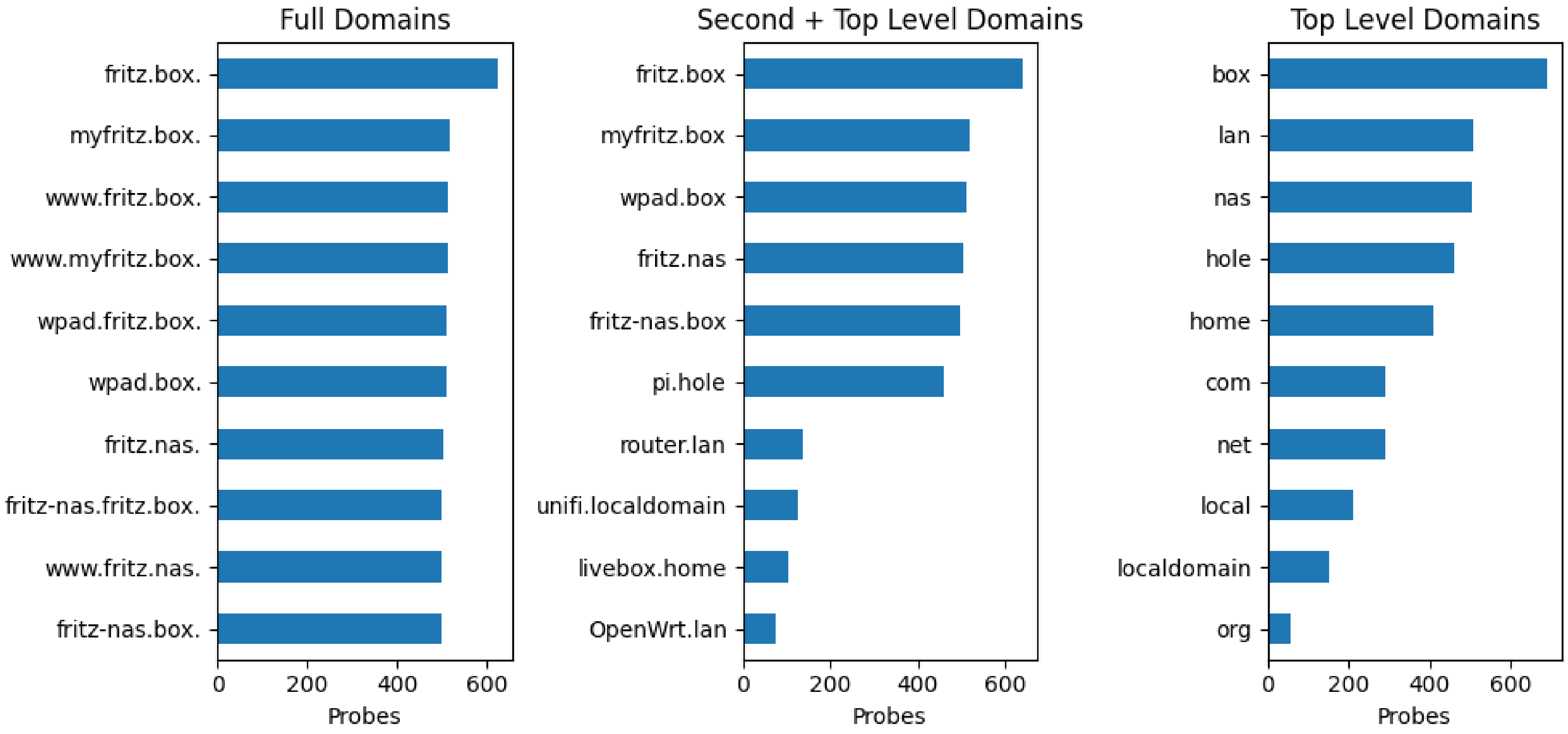
Measurement Setup

- How to detect internal names without prior knowledge?
- Get likely local address of the home gateway (using traceroute or DNS measurements)
- Send rDNS (IP address → name) queries for that address to get internal name
- Gateway fingerprinting step to find more probe using those names

Names Found

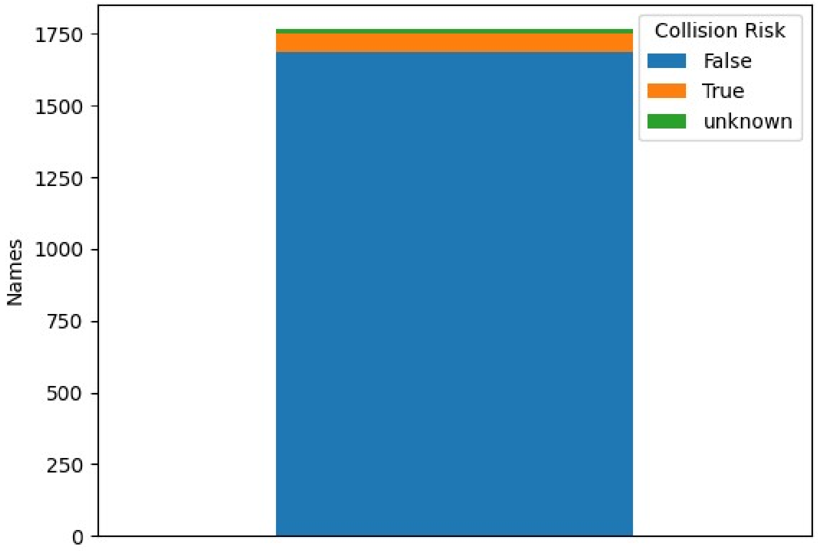
- Found **3092** names, used by **4305** probes
- 4203 probes (97.63%) found an rDNS record for the internal name
- 102 additional probes found through fingerprinting step

Names Found


Full Domains
fritz.box.
myfritz.box.
www.fritz.box.
www.myfritz.box.
wpad.fritz.box.
wpad.box.
fritz.nas.
fritz-nas.fritz.box.
www.fritz.nas.
fritz-nas.box.
0
200
400
600
Probes
Second + Top Level Domains
fritz.box
myfritz.box
wpad.box
fritz.nas
fritz-nas.box
pi.hole
router.lan
unifi.localdomain
livebox.home
OpenWrt.lan
0
200
400
600
Probes
Top Level Domains
box
lan
nas
hole
home
com
net
local
localdomain
org
0
200
400
600
Probes

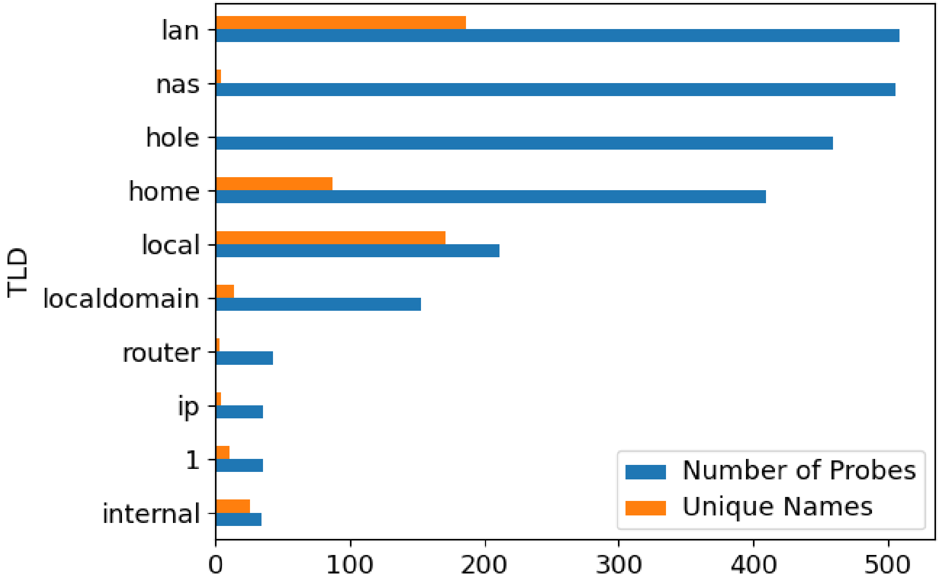
Current Collision Risk

- 1766 names (57.12%) have a TLD in the DNS
- How many names could be registered today?
- Only 2.13% of all names



Non-public TLDs

- 42.88% of names have a TLD that is not in the public DNS
- 34.51% are **not** a subdomain of a special-use domain name → TLD could be added to the DNS in the future
- Low risk for .home and .internal, higher for the others
- .nas (another FRITZ!Box TLD) is common



Next Steps

- Networks found on RIPE Atlas might not be representative, possible alternative approaches:
  - Using the JavaScript from online advertisements to perform global measurements
  - Scanning the IPv4 address space to detect gateways that reveal internal names to the outside

Conclusions

- Wide variety of internal names, but FRITZ!Box related names are common

- Low current risk of name collision

- ~34% of names are at risk if their TLD is delegated

Elizabeth Boswell

University of Glasgow

e.boswell.2@research.gla.ac.uk

https://www.gla.ac.uk/pgrs/elizabethboswell/