Two Sides of the Shield: Understanding Protective DNS Adoption Factors

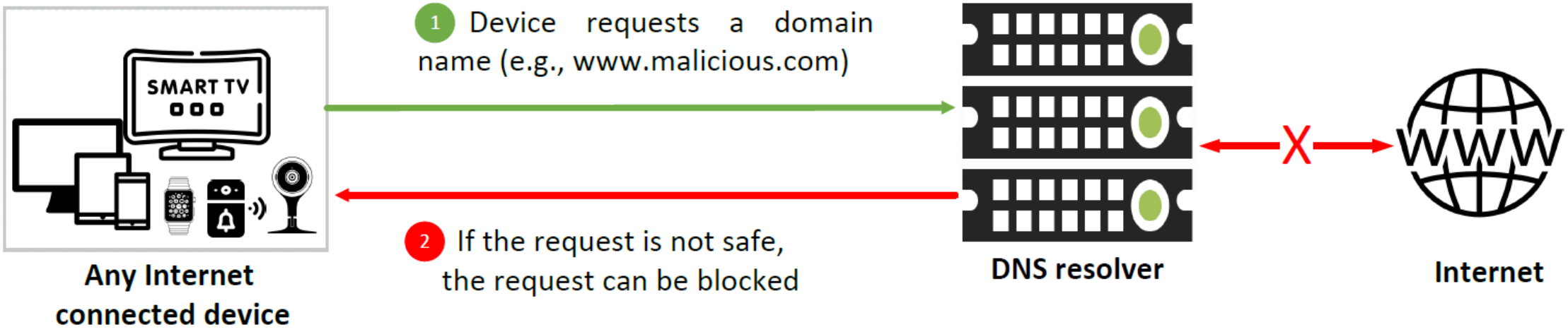
Elsa Rodríguez, Radu Anghel, **Simon Parkin**, Michel van Eeten, Carlos Gañán

Delft University of Technology

Emergence of Protective DNS (PDNS)

- Domain Name System (DNS) resolvers beginning to filter malicious content
  - Block known malicious domains -> **Protective DNS**
- Government-level PDNS schemes are emerging
  - UK, Canada, US, Australia; EU announced plans
- Switching to govt-level PDNS prevents service providers from monitoring threats
- The question is, **do users and enterprises want PDNS?**
  - Commercial and strategic PDNS programmes are moving ahead, yet … this has not been asked yet!

What is Protective DNS?



- **Technology functionality** – filtering requests to sets of addresses
- **Security benefit** – how it fits with the security of the device(s)
- **Service management** – where the DNS resolver is and who operates it

Research Questions

What is the extent of adoption of public DNS and, in particular, PDNS?

What factors encourage or discourage the adoption of Protective DNS by users and organizations?

Methodology – Multi-method

1. Actual adoption
2. Home-user Adoption Factors
3. Home-user Adoption Opportunities
4. Enterprise Adoption Factors
5. Expert interviews

Methodology – Multi-method

Actual Adoption	• PDNS use - Asia Pacific Network Information Centre (APNIC) daily DNS measurement • Measured 240 countries/territories
Home-user Adoption Factors	• Prolific Survey: 295 users, 29 countries, measure DNS resolver • Explain PDNS -> Ask about own perceived vulnerability; skills; PDNS effectiveness; willingness to adopt; comparable controls; who should manage PDNS
Home-user Adoption Opportunities	• ISP customer interviews: 25, from 284 ISP customers • perceived vulnerability, existing controls, PDNS effectiveness

Methodology – Multi-method (2)

Enterprise Adoption Factors	• Interviews 12 professionals responsible for threat response in organizations • Ask about awareness of PDNS, pros and cons
Expert interviews	• Nine members of Regional Internet / RIPE DNS mailing list • What PDNS is, pros and cons of PDNS, thoughts on government-level initiatives

Findings – APNIC data

What is the extent of adoption of public DNS and, in particular, PDNS?

Adoption of PDNS is low, ranging from 0.8% to 2% across regions

Table 1: DNS Resolvers Usage (Period: January to June 2022)

		Non Public DNS resolvers			Public DNS resolvers				
Region	**avg daily queries**	**% Same AS**	**% In country**	**% Out country**	**% PDNS**	**% Possible PDNS**	**% No PDNS**	**% No Info**	**Total**
Africa	1,671,192	58.2%	9.3%	1.2%	2.0%	2.0%	26.0%	1.3%	100%
Oceania	73,443	83.0%	5.3%	1.3%	1.0%	2.3%	7.0%	0.1%	100%
America	2,804,980	65.0%	9.2%	1.3%	0.9%	3.1%	20.2%	0.3%	100%
Europe	1,758,927	75.2%	7.6%	1.0%	0.9%	3.2%	12.0%	0.1%	100%
Asia	9,023,027	59.0%	20.0%	1.0%	0.8%	2.0%	17.0%	0.2%	100%

Findings

What factors encourage or discourage the adoption of Protective DNS by users and organizations?

Findings – Survey + ISP customers

- 121 participants had not heard of PDNS – many positive about it
- Motivators for adoption: own perceived vulnerability + perceived usefulness (and value) of service
- Cost was a significant factor
- Provider has biggest role: 156 (53%) chose ISP (logical choice), 100 a commercial provider (market forces), 24 their govt
- ISP interviews similar – low opt-in as other controls seen to suffice; ISP should be capable and trustworthy

Findings – Enterprise interviews

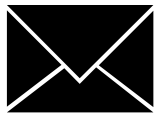
- **Reasons to implement PDNS**
  - Global Threat Intelligence sharing, ease of implementation
  - Extra layer of (strategic) security
- **Factors to consider for adoption (for those without PDNS)**
  - Cost; effectiveness; complementarity to current infrastructure
- **Concerns of adopting the service**
  - False positives; transparency of service as to what is blocked; privacy and trust in provider
- **Caveats about government PDNS initiatives**
  - Good if free and with freedom in configuration, and commercial value-adds (as above)

Findings – Experts interviews

- **Awareness:** call for (home) users to understand PDNS
  - What is blocked, how data is handled
- **Fit is important for adoption:** PDNS efficiency, organization's threat model + values, cost
- **Utility of PDNS:** perceived usefulness + perceived vulnerability (threat model) are important
- **Logical nature of an ISP role:** transparency concerns if govts block benign addresses

Summary

- Users/customers, enterprises, and experts prioritise privacy, trust, and transparency
- Role of PDNS provider is critical
  - Users prefer ISPs, and their government the least
  - PDNS complements other controls, but difficult to distinguish
- Subsidizing ISP PDNS for users is an alternative for govts
- Blocklist sharing a possible alternative for organizations

 s.e.parkin@tudelft.nl