Overview

- **RFC7626** published in August 2015 (first DPRIVE doc)

- Abstract: “This document describes the privacy issues associated with the use of the DNS by Internet users. It is intended to be an analysis of the present situation and does not prescribe solutions.”
Overview

- **RFC7626** published in August 2015 (first DPRIVE doc)

- Abstract: “This document describes the privacy issues associated with the use of the DNS by **Internet users**. It is intended to be an analysis of the present situation and does not prescribe solutions.”

1. Limited to privacy (not security or trust or network/operator)
2. It was a snapshot - described only the typical deployment of DNS at the time
Why a bis?

• Before any new DPRIVE WG & DoH WG standards, only discusses cleartext - things have changed!

• Best Current Practices for DNS Privacy operators
  - latest version is based on threat/mitigation model

• An updated RFC7626 seemed like the right place to describe new threats (companion document)
  • **Threats:** RFC7626-bis
  • **Mitigations:** draft-ietf-dprive-bcp-op
Document status

- Jul 2018: Published -00
- Jan 2019: Updated to -01, only minor updates
- Mar 2019: Call for adoption started yesterday - thanks for comments!
What’s new in the bis?

• Add new work (DoT(D)/DoH), standards and deployment.
• Update many references.
• Add section: DNS payload content (ECS, DNS Cookies, etc.)
• Attacks on encrypted transports, potential for tracking via transport
• In the server: analysis of DoT and DoH (headers)
• Authentication of servers
• Blocking of encrypted services
What’s still missing or needs work?

• Is DoT/DoH covered sufficiently?
• Should the scope of this document be expanded?
  • Trust model of provider
  • Security of discovery/config mechanisms
• Would this move to another WG if one was formed to focus on policy/deployment….?
Questions?