Why Host Encrypted DNS Forwarders on managed CPEs ?

IETF 119

March 2024

Tiru Reddy (Nokia)

M. Boucadair (Orange)

Dan Wing (Citrix)

Shashank Jain (McAfee)

The Problem

- Goal: Deploy encrypted DNS on local managed CPEs
  - Improve privacy: local network, query aggregation
  - Improve security: malware filtering, MUD [RFC8520]
  - Improve performance: Local DNS caching
  - Preserve User Experience: Provide local services
- Need Secure CPE (Discussed in Slides 3, 4 and 5)
- However,
  - Encrypted DNS requires CA-signed certificates
  - Difficult to obtain CA-signed certificates for CPEs
  - Managed CPEs ease user burden, but creates scale burden

Modern Managed CPE

- Already support encrypted DNS (e.g., PowerDNS DNSdist).
  - https://blog.open-xchange.com/dnsdist-as-a-router-ready-solution

- Network security services on secure home routers (e.g., hardened OpenWRT)
- Offered by several security vendors, McAfee, SAM, Trend Micro, etc.
- Millions of secure CPEs deployed today.

Security Requirements Met by CPEs

- Security measures for Device Management
  - Patch management and update policy (Upgraded without end-user intervention)
  - Secure transport mechanisms
  - Certificate Management
  - Data encryption
  - Secure Firmware/Software Update
  - Secure Device Management

Security Requirements Met by CPEs

- Vulnerability Management
- Exploit Mitigations
  - Runtime Integrity
  - Microservices/Containers
- Prpl Foundation adds on carrier-grade security, software hardening, QA and testing:
  - https://prplfoundation.org/wp-content/uploads/2018/04/prpl-Device-Security-Requirements-v1.0.pdf

Do53 over WPA3: Insecure

- WPA3 offers security for Wi-Fi networks
- Multiple network devices between the endpoint and network entity hosting the encrypted forwarder:
  - Encrypted DNS ensures only the network entity (e.g., Mesh Gateway) hosting the forwarder has visibility into the DNS traffic
- DNS clients may not know about WPA3 and if the DNS resolver is co-located on the WPA server

DNR/DDR

- DDR's scope is restricted to public IP addresses
  - Prefix re-numbering induces issues
    - DNS service delayed until that new certificate is acquired
  - ACME IP Identifier Validation Extension (RFC 8738) not supported by CAs
- DNR requires proving possession of an FQDN
  - Unique FQDNs are viable (e.g., cpe1.example1.com)
    - HTTPS Access to the Home Router
  - ACME approach: CPE hosts Internet-facing HTTP or DNS server
    - Struggle with CGN (mobile networks)
  - An Alternative: CPE obtains certificate signature from Internet-facing server

Issuing CPE Certificates from CAs

- Dependency in CAs to issue certificates for millions of CPEs
- Could trigger DoS mitigation (throttling) by CA
  - When a large scale of CPEs request certificate issuance for many subdomains, it could be treated as an attacker by the certificate authorities to overwhelm it
- Ongoing traffic to renew short-lived certificates (STAR, RFC8739). It is yet to be seen if CAs will agree to support star certificates at a scale of millions of CPEs

Potential Solution: Avoid High Traffic to CAs

- Send traffic to Managed CPE service (rather than CA)
- Use *subcerts* [RFC9345] or *name constraints* [RFC8280]

subcerts	**name constraints**
• Con: TLS client & server need subcert support • Pro: Some client support (Firefox)	• Standardized 2008 • Con: Little/none CA support. CA Browser form does not encourage it. Auditing