Hosting Encrypted DNS Forwarders Servers on CPEs

draft-rbw-add-encrypted-dns-forwarders

IETF 120
July 2024

Tiru Reddy (Nokia)
M. Boucadair (Orange)
Dan Wing (Citrix)
ADD: TLS for DNS on CPE

• Deployed: CPE gets CA-signed certs from a vendor-operated cloud service
  – Each CPE gets unique host name (SAN)
    • cpe-5837.example.com similar to unique SSID
  – McAfee CPE, Mozilla IoT Gateway, Cujo CPE

• Problem: Certificate Authorities unhappy to sign millions of certificates
Conclusion of IETF119 ADD

• Problem is bigger than ADD
• Encrypted DNS is like other in-home encrypted services
  – TLS for DNS ← ADD is here
  – HTTPS for CPE management
  – SMB over QUIC
  – Printer (IPP over TLS)
  – Internet of Things
  – Etc.
Discussion

• Identification: unique name rather than IP
• Authentication: CA-signed certificates
  – Normal CA-signed certificates (deployed today)
    • CA unhappy to sign millions
  – Short-lived certificates (STAR, RFC8739)
    • Unknown CA support for millions
  – Name Constraints (RFC5280 §4.2.1.10)
    • No/little CA support

https://tinyurl.com/https-for-local-domains
Next Steps

• Co-authors for problem statement document
BACKUP SLIDES
SECURING CPE
Modern Managed CPE

• Already support encrypted DNS (e.g., PowerDNS DNSdist).

• 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 measures for Device Management

• Patch management and update policy (Upgraded without end-user intervention)
• 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:
Achieving Encrypted DNS

- **WPA3**
  - Wi-Fi only
  - Client cannot ensure encrypted path

- **TLS**
  - Wi-Fi and Ethernet
  - End to end encrypted path
CERTIFICATES FOR DNR
CPE Certificate

Both allow client to identify and authorize the Encrypted DNS server

<table>
<thead>
<tr>
<th>Self-Signed</th>
<th>CA-signed</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Certificate warnings</td>
<td>• Authenticated</td>
</tr>
<tr>
<td></td>
<td>• Can also provide HTTPS for CPE management console</td>
</tr>
</tbody>
</table>
DDR: prove possession of IP

• DDR’s scope is restricted to public IP addresses
  – IP re-numbering creates issues
    • DNS service delayed until new certificate is acquired
  – Struggle with IPv4 CGN (5G hotspot)
• ACME IP Identifier Validation Extension (RFC8738) not supported by CAs
• Poor user experience (“2001:db8:6:7::9 is mine!”)
DNR: prove possession of FQDN

• Unique FQDNs are viable (e.g., cpe123.example.com)

• ACME approach: CPE hosts Internet-facing HTTP or DNS server
  – Struggle with CGN (5G hotspot)

• Deployed today: CPE obtains certificate signature from Internet-facing server

• Client policy can allow named certificate for DNR
Scaling CA Signing

• Dependency on CAs to issue millions of certificates
• Could trigger DoS mitigation (throttling) by CA
• Need agreement to avoid throttling
Other Potential Solutions

• Avoid high traffic to CAs by using *Name Constraints* (RFC5280)
  – Standardized 2008, but little/no CA support

• Periodically renew short-lived certificates (STAR, RFC8739)
  – STAR certificates require CA support
  – Unknown if CAs will support STAR certificates for millions of CPE
Document Scope

• Discuss Goal, Problems, and Solutions