Ochrana soukromí v DNS

Ondřej Caletka

cesnet

31. ledna 2019

cesnet

Best Current Practice #188

Internet Engineering Task Force (IETF) S. Farrell
Request for Comments: 7258 Trinity College Dublin
BCP: 188 H. Tschofenig
Category: Best Current Practice ARM Ltd.
ISSN: 2070-1721 May 2014

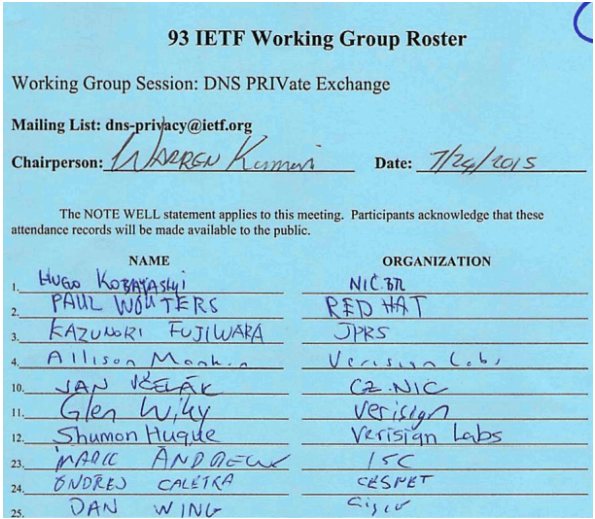
Pervasive Monitoring Is an Attack

Abstract

Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible.

cesnet

Vznik pracovní skupiny DPRIVE



93 IETF Working Group Roster

Working Group Session: DNS PRIVate Exchange

Mailing List: dns-privacy@ietf.org

Chairperson: Warren Kumari **Date:** 7/24/2015

The NOTE WELL statement applies to this meeting. Participants acknowledge that these attendance records will be made available to the public.

	NAME	ORGANIZATION
1.	Hugo Kobayashi	NIC.BR
2.	PAUL WOUTERS	RED HAT
3.	KAZUNORI FUJIWARA	JPRS
4.	Allison Mankin	Verisign Labs
10.	JAN VČELÁK	CZ.NIC
11.	Glen Wiley	Verisign
12.	Shumon Huque	Verisign Labs
23.	MARC ANDRIESEN	ISC
24.	ONDŘEJ CALETKA	CESNET
25.	DAN WING	Cisco

- ustavena v roce 2014
- cílem je ochránit důvěrnost DNS zpráv
- primárně mezi koncovým systémem a resolverem

cesnet

Opravdu potřebujeme nový protokol?

- už mnoho let máme IPsec
- je možné ho nakonfigurovat pro oportunistické šifrování
- může šifrovat jen DNS, nebo veškerý provoz s danou adresou
- potřebujeme tedy vůbec nový *VPN protokol* jen pro DNS?

cesnet

Opravdu potřebujeme nový protokol?

- už mnoho let máme IPsec
- je možné ho nakonfigurovat pro oportunistické šifrování
- může šifrovat jen DNS, nebo veškerý provoz s danou adresou
- potřebujeme tedy vůbec nový *VPN protokol* jen pro DNS?

No jasně, že ano! A hned dva!

cesnet

Populární a nepopulární protokoly

cesnet

Populární a nepopulární protokoly

Nepopulární

- IPv6
- DANE
- DANE
- IPSEC
- DNSSEC

Populární

- IPv4 + NAT + PAT + ALG
- CAA záznamy
- ACME + Let's Encrypt
- TLS
- Split horizon DNS

cesnet

Prostě to protunelujeme

RFC 7766: DNS-over-TCP

- TCP může být protokolem první volby
- TCP spojení může být použito opakovaně
- dotazy je možno řetězit, server může vyřizovat paralelně
- diskuze o TCP Fast Open

RFC 7858: DNS-over-TLS

- TLS tunel na portu tcp/853
- oportunistické i vynucené šifrování
- volitelná autentizace pomocí key pinningu

cesnet

Podpora DNS-over-TLS

Servery

- Unbound
- Knot DNS resolver
- Cloudflare
- Quad9
- Google DNS

Klienti

- Android 9.0 Pie
- systemd-resolved
- Unbound
- Knot DNS resolver

cesnet

Vlastnosti DNS-over-TLS

- brání přinejmenším pasivnímu odposlechu
- lze na něj oportunisticky přejít
- autentizace DNS resolveru je problém
- port 853 lze snadno zablokovat
- resolver stále vidí veškerá data a může do nich zasahovat
- protokol lze použít k tunelování libovolných dat
- nešifrovaná DNS jména stále unikají v SNI hlavičkách TLS spojení

cesnet

cesnet

DNS over HTTPS

- pracovní skupina DoH ustavena v září 2017
- RFC 8484 vydáno v říjnu 2018
- posílání binárních DNS zpráv uvnitř HTTPS spojení
- předchozí implementace provozované Google a Cloudflare používající JSON
- dva režimy:
  - dedikovaný DoH server
  - DoH multiplexované s jinými webovými službami

cesnet

Vlastnosti DoH

- přítomno ve Firefoxu a Chrome (zatím skrytě)
- vyžaduje URL pro konfiguraci (DHCP nestačí)
- téměř nemožné zablokovat či kontrolovat
- DNS servery dostávají mnohem více metadat
- potenciál pro *resolverless* DNS – přenos autoritativních DNS dat přímo z WWW serveru
- experiment Firefox Nightly a Cloudflare
  - „Trusted Recursive Resolver“
  - výkonová penalta je nepatrná
  - problémy se split-horizon DNS

cesnet

Shrnutí

- DoT je jednoduchý upgrade stávající infrastruktury
  - už funguje v Androidu 9.0 Pie
  - zachovává moc nad DNS provozovateli sítě
  - lze snadno zablokovat externí resolvery
- DoH je poměrně kontroverzní revoluce
  - mění stávající pořádky
  - má velkou podporu vlivných lidí
- DNSSEC je ortogonální k oběma
  - zabezpečuje autenticitu dat end-to-end
  - může být nadbytečný pro *resolverless* DoH

cesnet

THE MOST POPULAR RESOLVER

TO ESTABLISH DOH SESSION
TO THE CLOUD RESOLVER

cesnet

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
https://**Ondřej.Caletka.cz**

Prezentace je již nyní k dispozici ke stažení.