Soukromí na Internetu

a převážně v DNS

Ondřej Surý • ondrej.sury@nic.cz • 2014 May 22

CZ DOMAIN REGISTRY

Snowdonia

Snowdenia

Pervasive monitoring

- Pervasive monitoring (PM) = všudypřítomné sledování
  - Využívání chyb v protokolech a implementacích
  - Zaznamenávání metadat (hlavičky, časování, ...)
  - Odposlouchávání linek (včetně optiky)
  - Pokud se dělá ve velkém měřítku, dají se data dávat do souvislostí

Pervasive monitoring is an attack

- IETF vydalo RFC7258, kde považuje za útok na soukromí na Internetu
  - PM je útok na soukromí na Internetu
  - Protokoly by měly obsahovat ochranu proti PM již v základu

Bezpečnost a soukromí v DNS

- Autenticitu DNS zajišťuje
  - DNSSEC – podepsané DNS záznamy (asymetricky, RRSIG)
  - TSIG – podepsaná DNS zpráva (symetricky, extra skrytý RR)
  - SIG0 – podepsaná DNS zpráva (asymetricky, extra skrytý RR)
- DNS protokol není šifrovaný (zatím)
  - dnscrypt (ehm)

Vyšší soukromí v DNS

- Dotaz na IN AAAA www.tlsa.cz
- Posílá se celý dotaz včetně typu na všechny DNS servery „po cestě”
  - a-m.root-server.org

    ```
    ;www.tlsa.cz.                IN      AAAA
    ```

  - a-d.nic.cz

    ```
    ;www.tlsa.cz.                IN      AAAA
    ```

  - pagan.rfc1925.org

    ```
    ;www.tlsa.cz.                IN      AAAA
    ```

Co s tím teď hned?

- Dotaz na IN AAAA www.tlsa.cz
- Posílá se jen nutné minimum
  - a-m.root-server.org

    ```
    ;cz.                    IN      NS
    ```

  - a-d.nic.cz

    ```
    ;tlsa.cz.               IN      NS
    ```

  - pagan.rfc1925.org

    ```
    ;www.tlssa.cz.          IN      AAAA
    ```

Šifrování v DNS

- Tak to teda zašifrujem, ne?
- dnscrypt
- DNSe BoF

DNSCRYPT – proč je to špatný nápad

- Hrozný hack nad DNS protokolem
- Veřejný klíč je zakódovaný do jména DNS serveru
- Data jsou šifrována do TXT záznamu
- Natvrdo zakódovaný (božský) algoritmus

DNSE BoF

- První setkání na IETF 89 v Londýně
- Pracuje se na definici problému
  - Soukromí...
  - Šifrování...
- draft-bortzmeyer-dnsop-dns-privacy

Šifrování v DNS

- Šifrování na nižší vrstvě
  - DTLS (něco jako HTTPS)
  - Vyžaduje handshake
- Šifrování v DNS zprávě
  - Vyžaduje přepracovat DNS protokol

Skrývání metadat

- Metadata obsahují také spoustu zajímavých informací
- Pouhé zašifrování nestačí
  - Délka zašifrovaných dat
    - www.nic.cz vs strasnedlouhyprefix.strasnedlouhadomena.cz
  - Dotazované autoritativní servery
    - Čím méně domén je na serveru,...
    - ...tím více dotaz prozradí

Další drobné problémy

- Musíme začít jinak přemýšlet!
- Jen zabezpečení DNS nestačí,...
  - ...pokud se pak dál připojuji nezabezpečeně
  - Ale také SNI není šifrované

Otázky

Zdroje

- Snowdonia photograph by Mike Peel (www.mikepeel.net).
- RFC7258: Pervasive Monitoring Is an Attack
- draft-bortzmeyer-dnsop-dns-privacy
- Caricature of villain by J.J.