# Novinky v DNS

## I dinosauři měli mladé

Ondřej Surý • ondrej.sury@nic.cz • 31.05.2016

CZ DOMAIN REGISTRY

# Co je nového v DNS?

- Knot Resolver 1.0.0
- Eliptické křivky pro DNSSEC
- DNS sušenky
- Minimizace QNAME
- DNS over TLS

# Knot Resolver 1.0.0

- Rekurzivní DNS server
- Svobodný software (GPL 3+)
- Vývoj podpořen firmou Comcast
  - Dojde k nasazení v průběhu letošního léta
- Plně skriptovatelné a rozšiřitelné jádro (C, Lua, Go)
- Podpora moderních DNS standardů s důrazem na soukromí a bezpečnost:
  - Automatická správa kořenů důvěry (TA) a negativní kořeny důvěry (TA)
  - QNAME minimization
- Připravujeme:
  - DNS Cookies
  - DNS over TLS

# Nové eliptické křivky v DNS

- SafeCurves(.cr.yp.to)
  - Daniel J. Bernstein a Tanja Lange
- Je rozdíl mezi bezpečností:
  - Elliptic-Curve Cryptography (ECC) ← obecně bezpečnost eliptické křivky
  - Elliptic-Curve Discrete-Logarithm Problem (ECDLP) ← problém, jak najít soukromý klíč z veřejného části
- ECDLP může být v pořádku, ale implementace může být špatná:
  - Implementace může poskytovat špatné výsledky pro některé výjimečné body na křivce
  - Implementace může vyzrazovat tajná data, pokud vstup není bod na křivce
  - Implementace může vyzrazovat tajná data pomocí časování větví v kódu
  - Implementace může vyzrazovat tajná data pomocí časování datové cache
- Kritéria SafeCurves jsou navržena tak, aby zajišťovala bezpečnost ECC a nikoli jen ECDLP

# Edwards-curve Digital Signature Algorithm (EdDSA)

- Schéma digitálního podpisu (varianta Schnorrova podpisu používající Twisted-Edwards křivky) s těmito vlastnostmi:
  - Vysoký výkon na různých architekturách a platformách
  - Nevyžaduje použití generátoru náhodných čísel pro každý podpis
  - Odolnost proti útokům přes boční kanály (časování, atp.)
  - Malé veřejné klíče (32 nebo 57 bajtů) a podpisů (64 nebo 114 bajtů)
  - Vzorce jsou “silně unifikované”, tj. jsou validní pro každý bod na křivce, bez výjimek. EdDSA tedy nemusí provádět náročnou validaci vstupních hodnot.
  - Odolnost proti kolizím, tj. kolize hašovací funkci nemají vliv na bezpečnost EdDSA

https://datatracker.ietf.org/doc/draft-irtf-cfrg-eddsa/

# RFC 7748 – SafeCurves v CFRG

- Curve25519 → Ed25519
  - 2006 Daniel J. Bernstein
  - ~128-bitová bezpečnost
- Curve448(-Goldilocks) → Ed448
  - 2014 Mike Hamburg
  - ~224-bitová bezpečnost

# SafeCurves v DNSSEC

- **draft-ietf-curdle-dnskey-eddsa**
  - Pracuje se na tom v CURDLE WG
  - Konsensus na použití Ed25519 a Ed448 pro DNSSEC
  - Aktuálně se řeší, co se Signature Context
  - A čeká se na finální verzi draft-irtf-cfrg-eddsa
- **draft-wouters-sury-dnsop-algorithm-update**
  - DNSSEC algoritmy jsou si rovny! Nebo jsou si některé rovnější?
  - Aktualizace použitelných a doporučených algoritmů pro DNSSEC
  - DSA a SHA1 musí jít, eliptické křivky jsou budoucnost
- **draft-york-dnsop-deploying-dnssec-crypto-algs**
  - Informativní draft o problémech s nasazováním nových algoritmů

# DNS Sušenky – Problém

- Neexistence filtrování odchozího provozu
  - Je snadné podvrhávat zdrojovou adresu
- DNS a jiné protokoly jsou používány pro:
  - DDoS
    - Hrubou silou ucpeme „trubky“
  - DNS DDoS
    - Zahlcení cílového DNS serveru, který zpracovává DNS pakety

# DNS Sušenky – Dietní řešení

- EDNS0 Option 10
  - Klientská sušenka
    - 8 bajtový (pseudo)náhodný řetězec
    - Unikátní pro každý DNS server (IP adresu)
  - Serverová sušenka
    - 8 – 32 bajtů
- DNS Sušenky poskytují (slabou) záruku, že klient není falešný

# Recept na DNS Sušenky

- DNS Klient nepošle sušenku
  - DNS Server se chová jako dříve

- DNS Klient pošle jen klientskou sušenku (nebo špatnou serverovou sušenku)
- DNS Server odpoví:
  - Normálně, a připojí novou serverovou sušenku
  - Přesměruje klienta na TCP
  - Odmítne odpovědět (dle response rate limiting)

- DNS Klient pošle klientskou a správnou serverovou sušenku
- DNS Server odpoví vždy, a buď:
  - Připojí sušenky z dotazu
  - Změní serverovou sušenku

# DPRIVE – DNS PRIVate Exchange

- RFC 7258 říká: „Všudypřítomné sledování je útok“
- Pracovní skupina DPRIVE vytváří mechanismy jak přidat do DNS transakcí soukromí
  - RFC 7816 – QNAME minimization
  - RFC 7858 – DNS over TLS
  - RFC 7830 – EDNS(0) Padding
    - Skrývání metadat

# RFC7816 – Minimizace QNAME

- Pro www.nic.cz IN A:
  - Pošli cz. IN A na kořenové servery
    - Dostaneme NS servery pro cz
  - Pošli nic.cz. na cz servery
    - Dostaneme NS servery pro nic.cz
  - Pošli www.nic.cz na nic.cz servery
    - Dostaneme celou odpověď

# RFC7816 – Minimizace QNAME

- Kompatibilita s reálným DNS světem:
  - Pokud v mezikroku dostaneme cokoli jiného než NOERROR, zkus to znovu s celým jménem
    - Workaround kvůli CDN (např. Akamai) a dalším rozbitým serverům
  - Pokud v mezikroku dostaneme odpověď místo odkazů na NS, připoj další label a zkus to znovu
  - Omezení na počet iterací
- Implementace:
  - Knot Resolver 1.0.0 – standardní chování
  - Unbound od verze 1.5.7, ale standardně vypnuto

# RFC7858 – DNS over TLS

- Dedikovaný port **853**
  - Kvůli různým „taky-firewallům“, co si myslí, že rozumí provozu na portu 53
- Určeno pro komunikaci (stub) klient ↔ resolver
- Naváže se TLS session a volitelně autentizuje
  - SPKI pinning
  - Opportunistic (pokud je dostupné, použije se)
- Implementováno:
  - Knot Resolver (tls-listen branch, bude v dalším stable release)
  - Unbound
  - getdns 0.1.8

# Díky za pozornost

**Ondřej Surý • ondrej.sury@nic.cz**