

DNCheck po roce provozu

Zonemaster

- AFNIC & The Swedish Internet Foundation
- kontroluje kvalitu DNS delegace
- přes 70 různých testovacích scénářů
 - DNSSEC
 - SOA, A, AAAA, MX, ...

Zonemaster

- podrobná dokumentace a popis všech testovacích scénářů
- výsledky testů: INFO, NOTICE, WARNING, ERROR, CRITICAL
- možnost vytvářet sady testů
- delegované i nedelegované testy

DNScheck

- nahradil staré technické kontroly
- nadstavba nad Zonemaster API
- automatické testování delegace všech domén v registru
- zasílání varování technickým kontaktům nssetu
- poskytujeme pomoc s opravou nastavení DNS

Zonemaster – úpravy

- nechceme se odchýlovat od výchozího nastavení
- cílem je případné změny propagovat do upstreamu
- DNSSEC03 – počet NSEC3 iterací > 0
 - RFC 9276 Guidance for NSEC3 Parameter Settings:
If NSEC3 must be used, then an iterations count of 0 MUST be used to alleviate computational burdens.
 - ve spolupráci s autory Zonemasteru ERROR $\Rightarrow$ WARNING

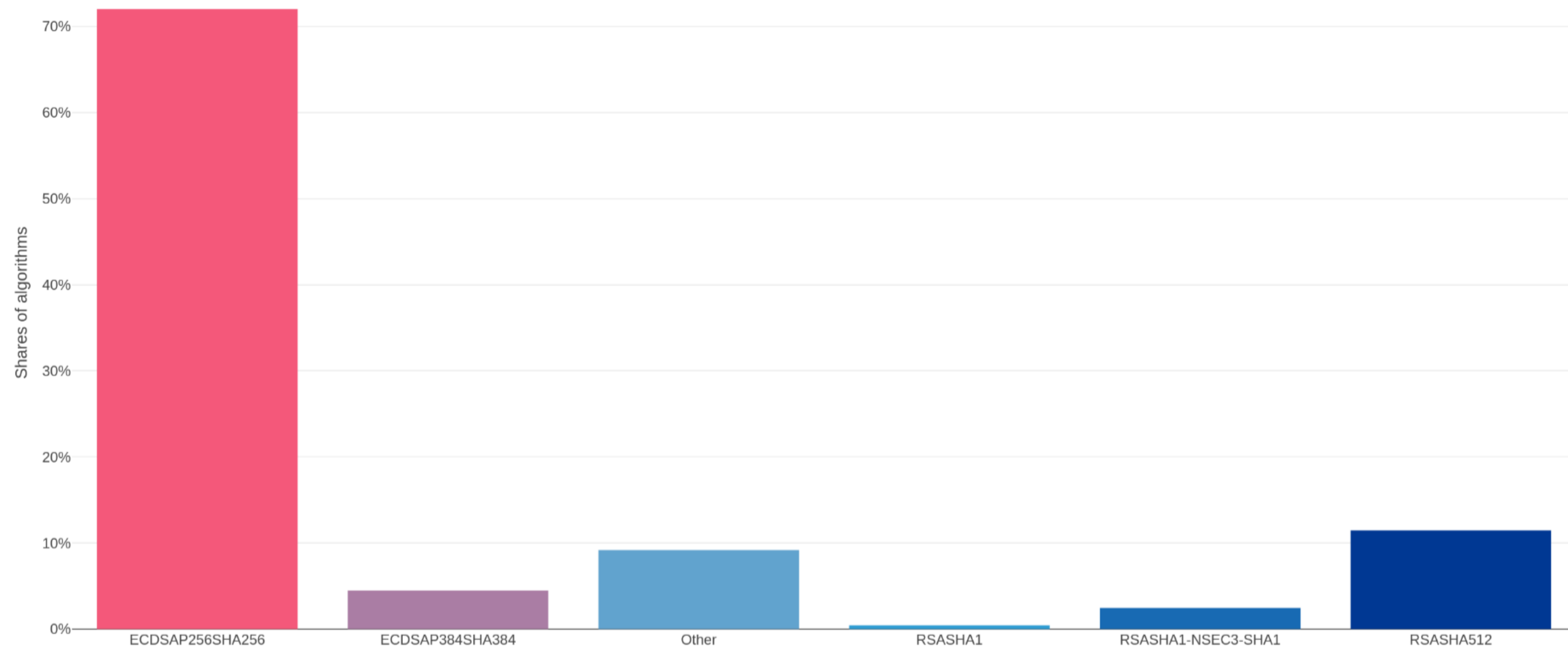
DNScheck – datová analýza

- celkový počet problémů významně neklesá
 - zaměříme se na problematické chyby a velké nssety
- závažné chyby
 - zastaralý algoritmus DNSSEC klíče
 - podepisování DNSSEC
 - nastavení NSEC3
 - chyby v nastavení nameserverů

Problém: DNSSEC algoritmy

Number	Description	Mnemonic	Zone Signing	Trans. Sec.	Use for DNSSEC Signing	Use for DNSSEC Validation	Implement for DNSSEC Signing	Implement for DNSSEC Validation
0	Delete DS	DELETE	N	N				
1	RSA/MD5 (DEPRECATED, see 5)	RSAMD5	N	Y	MUST NOT	MUST NOT	MUST NOT	MUST NOT
2	Diffie-Hellman	DH	N	Y				
3	DSA/SHA1	DSA	Y	Y	MUST NOT	MUST NOT	MUST NOT	MUST NOT
4	Reserved							
5	RSA/SHA-1	RSASHA1	Y	Y	MUST NOT	RECOMMENDED	NOT RECOMMENDED	MUST
6	DSA-NSEC3-SHA1	DSA-NSEC3-SHA1	Y	Y	MUST NOT	MUST NOT	MUST NOT	MUST NOT
7	RSASHA1-NSEC3-SHA1	RSASHA1-NSEC3-SHA1	Y	Y	MUST NOT	RECOMMENDED	NOT RECOMMENDED	MUST
8	RSA/SHA-256	RSASHA256	Y	*	RECOMMENDED	RECOMMENDED	MUST	MUST
9	Reserved							
10	RSA/SHA-512	RSASHA512	Y	*	NOT RECOMMENDED	RECOMMENDED	NOT RECOMMENDED	MUST
11	Reserved							
12	GOST R 34.10-2001 (DEPRECATED)	ECC-GOST	Y	*	MUST NOT	MUST NOT	MUST NOT	MUST NOT
13	ECDSA Curve P-256 with SHA-256	ECDSAP256SHA256	Y	*	RECOMMENDED	RECOMMENDED	MUST	MUST
14	ECDSA Curve P-384 with SHA-384	ECDSAP384SHA384	Y	*	MAY	RECOMMENDED	MAY	RECOMMENDED
15	Ed25519	ED25519	Y	*	RECOMMENDED	RECOMMENDED	RECOMMENDED	RECOMMENDED
16	Ed448	ED448	Y	*	MAY	RECOMMENDED	MAY	RECOMMENDED

Problém: DNSSEC algoritmy



- zastaralý algoritmus
- krátký klíč (např. RSA/SHA-256 s 1024 bitovým klíčem)

Problém: Podepisování DNSSEC

- zóna je podepsaná, ale chybí DS záznam
- zóna má DS záznam, ale není podepsaná
- *může se objevovat i u rušených zón*

Problém: Nastavení NSEC3

- dle RFC 9276 nastavení prázdné salt a iterací na 0
- iterace přenášejí výpočetní složitost na resolvery
- usnadnění DoS útoků

Problém: Nastavení DNS nameserverů

- minimální počet 2 NS pro IPv4 i IPv6
- chyby
 - NS neodpovídá na zónu
 - NS ukazují na CNAME
 - NS záznamy směřují na stejnou IP adresu (nebo IP ze stejného rozsahu)
 - NS záznamy neodpovídají těm v nadřazené zóně
 - MX záznam ukazuje na CNAME
 - autoritativní NS je rekurzor

DNScheck - budoucnost

- budeme dál skenovat celý registr a sbírat data
- návody ke správnému nastavení nameserverů a DNSSEC
- komunikace ohledně správných nastavení se správci nssetů
- zvážíme úpravu zasílání notifikací

Děkuji za pozornost