DNSSEC v distribuci Fedora

Red Hat, Inc.

Adam Tkáč, atkac@redhat.com

04.06.2009

fedora

Rekurzivní servery

- nejsnadnější cíle, široký dopad úspěšného útoku
- složitá správa a aktualizace bodů důvěry před podepsáním kořenové domény
- automatická aktualizace vyžaduje podporu od správců domén (RFC 5011)
- nutnost přesného času
- omezený výkon DLV registrů

fedora

Distribuce může správu zjednodušit

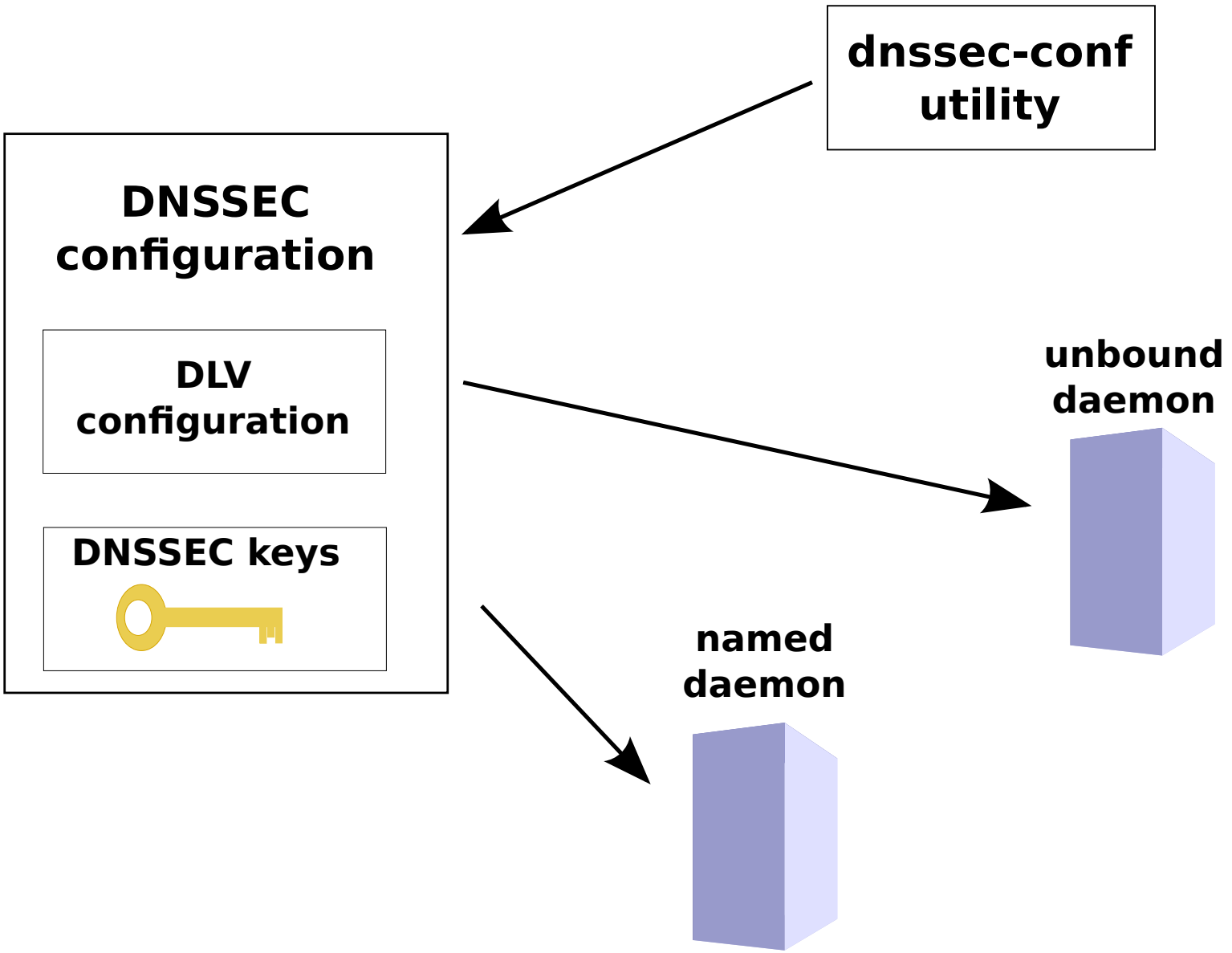
- automatická aktualizace klíčů
- centralizovaná správa
- integrace jednotlivých serverů, jednotné nastavování DNSSEC
- možné problémy
  - nedostatečné ověřování klíčů distributorem
  - instalace distribuce se starými klíči
  - zotavení, pokud nebyly klíče dlouho aktualizovány

fedora

Integrace v distribuci Fedora 11

- adresář /etc/pki/dnssec-keys/ obsahuje klíče pro všechny TLD, které provozují DNSSEC
- centralizovaná konfigurace v /etc/sysconfig/dnssec
- integrovány servery BIND a unbound
- servery mají ve výchozím nastavení zapnutou validaci pro domény, kde je DNSSEC v produkčním nasazení
- povolena DLV, používán registr společnosti ISC
- vše v balíčku "dnssec-conf"

Integrace - pokračování



fedora

Klientské stanice

- integrace DNSSEC do současných "stub" resolverů je nevhodná
  - duplikace kódu, plýtvání časem
  - dohadování se s "upstreamovými" vývojáři
- jsou také rekurzivními servery
- měly by se dotazovat pouze serverů, které provozuje jejich ISP
- plně automatická správa
- jednoduché vypnutí validace

fedora

Integrace na klientských stanicích

- jako přijatelné se rýsují dvě možnosti
- NetworkManager
  - dynamicky reaguje na změny na síti
  - je nutno vyvinout knihovnu, která zpřístupní potřebné informace (DNS servery, lokální domény, síťová rozhraní, ...)
  - podle poskytnutých informací se nakonfiguruje rekurzivní server
- DHCP hooks
  - lze použít v situacích, kdy neběží NetworkManager
  - skript nastaví rekurzivní server podle informací z DHCP
- neexistuje plán, kdy bude podpora v distribuci (Fedora 13?)

fedora

Možné problémy uživatelů

- chybné síťové prvky a middleware
  - "nejede Vám DNS? Kupte si nový router!"
- expirace klíčů; uživatel neaktualizuje, instalace starší distribuce
- při podvržení jména se zdá, že "nejede Internet"
- delší doba prvního překladu jména
- spouštění více služeb při startu systému (named/unbound, ntpd)

fedora

Přínosy integrace DNSSEC

- sklizeň plodů více než desetileté práce internetové komunity
- zabezpečení klíčové služby síťové infrastruktury
- uživatelé budou "v bezpečí"
- cachování záznamů na straně klienta; rychlejší odezva, nižší zátěž sítě
- snadné používání různých DNS serverů pro různé domény (připojení do více VLAN apod)

Dotazy?

Děkuji za pozornost.