AUTOMATIC TRACKING OF DNSSEC CONFIGURATION ON DNS SERVERS

Radek Lát
Bachelor Degree Programme (3), FIT BUT
E-mail: xlatra00@stud.fit.vutbr.cz

Supervised by: Petr Matoušek
E-mail: matousp@fit.vutbr.cz

Abstract: This paper describes design and implementation of a tool for tracking of configuration of DNSSEC security extension on DNS servers. The goal is to perform automatic verification of signatures, tracking of cryptographic algorithms being used and inform about potential or found problems. This tool has been developed in cooperation with CZ.NIC association.

Keywords: Secure DNS, DNSSEC, chain of trust, verification, signature

1. ÚVOD

DNS byl navržen jako hierarchický systém sloužící zejména pro překlad doménových jmen na IP adresy. Na bezpečnost však nebyl kladen velký důraz. S přibývajícími útoky na tento systém vyvstala potřeba zabezpečení tohoto protokolu, a to zejména z hlediska ověření původu a integrity dat.

Prostředkem k dosažení takového ověření je rozšíření protokolu DNS s technikou DNSSEC [1], která k tomu účelu využívá nové druhy záznamů (NSEC, NSEC3) a digitální podpisy dat (záznamy RRSIG, DNSKEY, DS), přičemž zachovává zpětnou kompatibilitu se stávajícím systémem DNS [2]. Pokud mají být záznamy skutečně zabezpečené, je potřeba pravidelná údržba dat na samotných DNS serverech, např. kontrola platnosti podpisů apod.

Nástroj, jehož návrh a implementace je popsána v tomto dokumentu, slouží k ulehčení pravidelné údržby pomocí procházení zón se zabezpečenými DNS záznamy, kontroly platnosti podpisů, upozorňování na neoptimální či nedostatečná bezpečnostní opatření, generování statistik a dalších informačních výstupů.

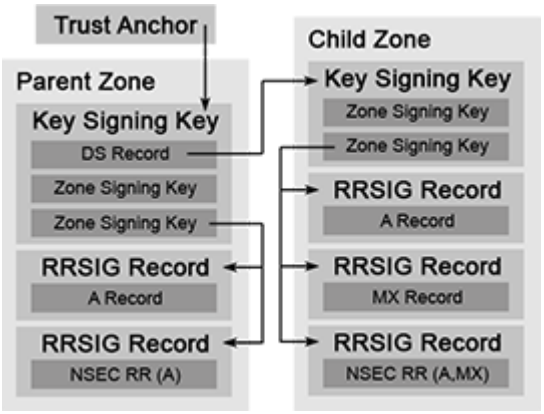
2. PROBLÉMY PŘI VERIFIKACI

Způsob zabezpečení pomocí DNSSEC je k vidění na obr 1**Chyba! Nenalezen zdroj odkazů.**. K podpisu záznamů se využívá Zone Signing Key (ZSK), k podpisu ZSK se využívá Key Signing Key (KSK) a na ten se odkazuje z rodičovské zóny pomocí DS záznamů, které jsou opět podepsány pomocí jiného ZSK klíče. Pro ověření podpisu je potřeba vytvořit řetěz důvěry sestávající se z posloupnosti DS záznamů a klíčů (KSK, ZSK, Trust Anchor). Tvorba řetězu tedy vyžaduje potřebu komunikace s rodičovskými zónami. Získávání jednotlivých záznamů ze všech zón a získání ověřených klíčů pro možnost kontroly podpisů je tedy netriviální.

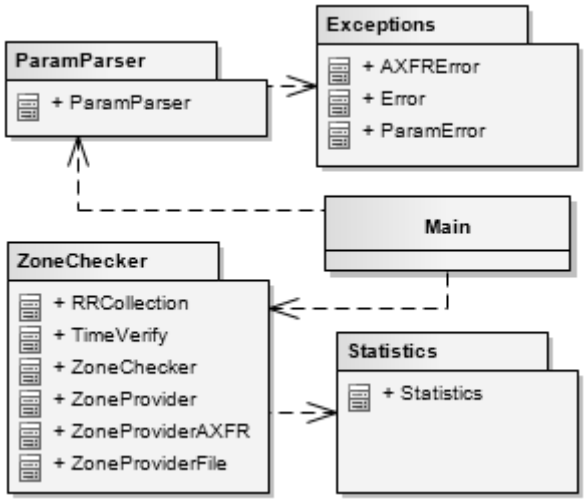
Pro ověření podpisu je potřeba nejprve vytvořit otisk (fingerprint) ze všech položek podepsaného záznamu seřazených za sebou, a ten porovnat se získaným rozšifrovaným otiskem z podpisu. Otisk je jinými slovy hash, tedy výstup určité hashovací funkce použité na data podepsaného záznamu. Různé druhy záznamů obsahují různé počty a druhy položek a existuje přes 60 druhů záznamů [3]. Pro zaručení možnosti ověření každého z nich by byla nutná databáze těchto formátů, která by se musela průběžně aktualizovat.

Stejný problém platí i pro algoritmy používané pro vytváření otisků. V současné době je možné použít několik různých typů a v budoucnu budou přibývat další. Byla by opět nutná nějaká databáze funkcí pro vytváření otisků.

Všechny tyto a některé další problémy lze úspěšně a relativně snadno vyřešit pomocí jediné knihovny, jak bude ukázáno níže.



Obr. 1- Schéma podpisů



Obr. 2 - Moduly a třídy aplikace

3. NÁVRH APLIKACE

Aplikace je implementována v jazyce Python. Využívá funkce pro práci s DNS, včetně jeho rozšíření DNSSEC, které poskytuje knihovna ldns [4] a její wrapper pro python s názvem PyLDNS. Výsledný nástroj funguje ve formě konzolové aplikace, umožňuje tedy konfiguraci pomocí parametrů předaných z příkazové řádky nebo pomocí konfiguračního souboru. Při návrhu a implementaci jsem využil objektový návrh a jednotlivé moduly jsou koncipovány tak, aby je bylo možné použít jako knihovny v jiných aplikacích. Seznam modulů, jejich tříd a provázání jednotlivých modulů v rámci aplikace je k vidění na obr. 2.

3.1. MODUL ZONECHECKER

Tento modul je funkčním jádrem aplikace. Třída ZoneChecker využívá dalších dvou tříd – TimeVerify pro ověřování časové platnosti podpisů a RRCollection, která umí seskupovat záznamy s jejich odpovídajícími RRSIG a NSEC/NSEC3 záznamy do jediného objektu. Ve velké míře je zde také využita knihovna PyLDNS.

První z hlavních funkcí je možnost postupného načítání obsahu celé zóny ze zónového souboru, kterou poskytuje třída ZoneProviderFile. Je též možné načítání dat pomocí zone transferu (i zabezpečeného pomocí TSIG) pomocí třídy ZoneProviderAXFR. Dále umožňuje načítání vlastních klíčů, které jsou považovány za důvěryhodné. To je užitečné v případech, kdy je zóna tzv. „island of trust“. Tento typ zóny vzniká v případě, kdy není možné ověřit zónu pomocí kořenového klíče. Neexistuje totiž řetěz důvěry od ověřované zóny až ke kořeni. Avšak taková zóna může být stale zabezpečená, pokud ověřující strana vlastní veřejné klíče dané zóny a získala je z bezpečného zdroje (nebyly podvrženy).

K vytváření řetězu důvěry je využita funkce `ldns_fetch_valid_domain_keys()` poskytovaná knihovnou PyLDNS, která dokáže celý řetěz důvěry sestavit, a poté vrací klíče, které bylo možné pro zadanou doménu ověřit. Pomocí těchto klíčů je pak možné ověřit podpisy záznamů pomocí funkce `ldns_verify_rrsig_keylist()`, která poskytuje možnost ověření všech aktuálních druhů záznamů pomocí všech používaných algoritmů.

Nakonec jsou přítomny funkce pro ověřování. Jsou rozděleny na samostatné ověřování podpisů, jejich časové platnosti, ověřování různých hodnot TTL, zda jsou vhodně zvoleny, také, zda má správnou strukturu a nakonec různé další doplňkové testy, které mají nízkou kritičnost, ale jejich výstup může být stále užitečný.

Důležitou funkčnost, která v knihovně PyLDNS chybí, obstarává funkce `__match_rrs()`, která při načítání obsahu zóny k jednotlivým záznamům přiřazuje jejich podpisy a NSEC/NSEC záznamy.

3.2. VÝSTUP NÁSTROJE

Pro výstup je využita knihovna logging, která jej umožňuje vytvářet snadno a jednotným způsobem. Formát výstupu je plně konfigurovatelný. Vyskytuje se v něm pět druhů zpráv, rozlišených podle své závažnosti: DEBUG, INFO, WARNING, ERROR a CRITICAL, kde první je nejméně závažná a poslední nejvíce. Následuje příklad výstupu:

2011-03-03 10:55:26 INFO: Signatures time check - example.com. - 6 total, 6 valid, 0 old, 0 future.

2011-03-03 10:55:26 DEBUG: Source file-example.com: Time signatures verified.

2011-03-03 10:55:26 CRITICAL: Source axfr-a.example.com: Can't start AXFR. Error: Could not send or receive, because of network error

na kterém lze vidět informační souhrn o kontrole časů platnosti podpisů, o úspěšně provedené kontrole a chybový stav, kdy nebylo možné získat obsah zóny pomocí zone transferu.

4. ZÁVĚR

Výsledný nástroj je využitelný pro správce zón a pro zóny libovolné velikosti. Na rozdíl od v současnosti dostupných nástrojů nemá omezení, plynoucí z načítání všech dat do paměti. Jediným omezením může být nemožnost kontrol zóny s náhodně uspořádanými záznamy. Nástroj však disponuje nastavitelnou vstupní vyrovnávací pamětí, pomocí které se dokáže vypořádat s částečnou neuspořádaností zóny. Nutno podotknout, že data v podepsaných zónách jsou obvykle vhodně uspořádána a proto se tento problém téměř nevyskytuje. Využití knihovny PyLDNS významně usnadnilo ověřování platnosti záznamů. Nástroj poskytuje rychlou možnost kontroly zóny, lze jej využít i k pravidelným kontrolám, jelikož si pamatuje sériová čísla ze SOA záznamů zón a lze jej nastavit tak, aby stejnou zónu nekontroloval dvakrát. Navíc je možné jeho libovolné rozšíření v budoucnu o další možnosti kontrol, jelikož tyto kontroly jsou striktně odděleny od zbytku programu. U nástroje se počítá s jeho nasazení pro kontrolu zón stravovaných organizací CZ.NIC v ČR. Zároveň by měl být ale k dispozici i pro jiné správce domén.

REFERENCES

[1] Arends, R., Austein, R., Larson, M., Massey, D., Rose, S., "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[2] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[3] *Iana : Internet Assigned Numbers Authority* [online].IANA, November 1987, 2011-02-22 [cit. 2011-02-27]. Domain Name System (DNS) Parameters. Dostupné z WWW: <http://www.iana.org/assignments/dns-parameters>.

[4] *NLnet Labs : ldns* [online]. Amsterdam : Nov 17 2010 [cit. 2011-02-27]. Dostupné z WWW: <http://www.nlnetlabs.nl/projects/ldns/>.