Projekt DNSSEC rozšíření pro Mozilla Firefox

Cílem toho projektu je vytvořit rozšíření pro prohlížeč Mozilla Firefox, který bude vizuálně informovat uživatele o bezpečnosti jeho připojení na základě protokolu DNSSEC. To umožní snáze identifikovat potenciální riziko podvrhu DNS záznamu při přístupu na internetové stránky a varovat uživatele. Rozšíření bude platformově nezávislé a volně k dispozici pod svobodnou licencí.

Používáné zkratky

DNS	Domain Name System
DNSSEC	DNS System Security Extensions
MF	Mozilla Firefox
XML	Extensible Markup Language
XUL	XML User Interface Language
JS	JavaScript
CSS	Cascading Style Sheets
XPCOM	Cross Platform Component Object Model
OARC	Operations, Analysis and Research Center
ODVR	Open DNSSEC Validating Resolver

Terminologie

V terminologii používané vývojáři MF se lze setkat s termíny „rozšíření“ (angl. extension), „zásuvný modul“ (angl. plugin) nebo „doplněk“ (angl. addon). Rozšíření typicky používá technologie XUL + JS + CSS a slouží k přidání nových funkcí, které prohlížeč standardně nenabízí. Zásuvný modul naopak využívá typicky technologie C/C++ a zajišťuje zobrazování/přehrávání multimediálních dat, jejichž podpora v prohlížeči chybí.

Z předchozího popisu je tedy zřejmé, že rozšíření je díky použití interpretovaných jazyků snadno platformově přenositelné, naopak zásuvné moduly jsou svou binární povahou silně platformově závislé.

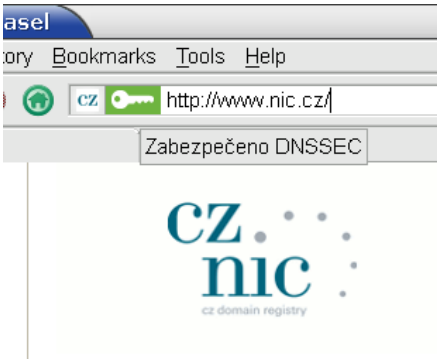
Naše řešení bude používat hybridní přístup, tzn. kombinaci všech výše uvedených technologií. Grafická část bude využívat interpretovaných jazyků, kdežto logika bude řešena jazykem binárním. Z tohoto pohledu je tedy vcelku jedno, zda výsledný „produkt“ bude nazýván rozšířením či zásuvným modulem. Pokud by však někdo chtěl být důsledný, pak jako nejvhodnější název zvolme „rozšíření s binárními komponentami“. Lze také použít název doplněk, což je obecné označení pro jakýkoliv přídavný kód do prohlížeče.

DNSSEC rozšíření pro Mozilla Firefox

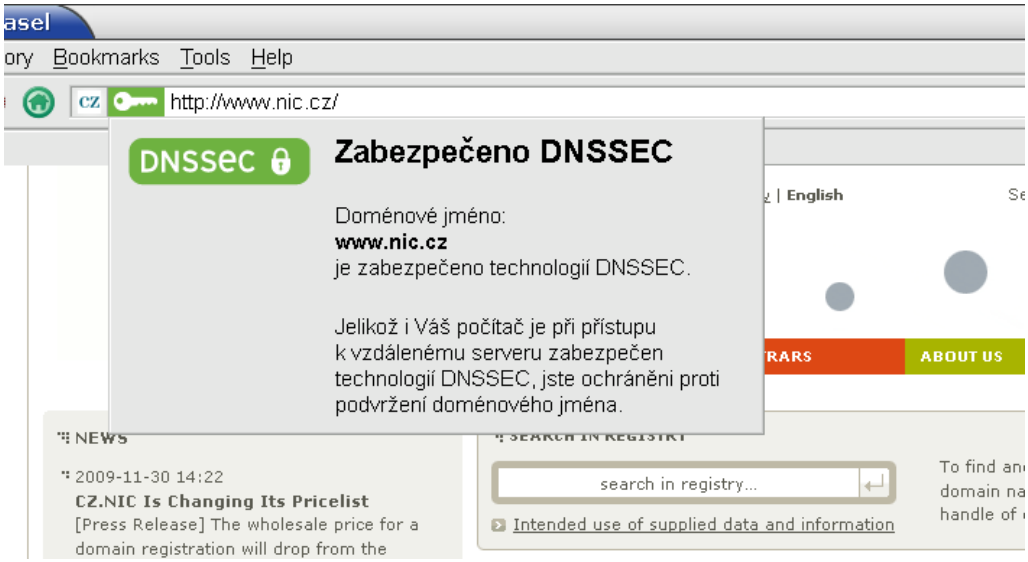
Specifikace

Grafické zpracování

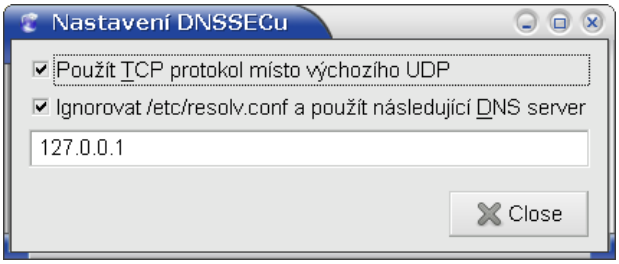
Rozšíření bude u webových stránek chráněných DNSSECem zobrazovat zelenou, oranžovou nebo červenou ikonku (tlačítko) klíče v závislosti na různých stavech připojení dle níže uvedeného stavového diagramu. U nechráněných stránek se ikonka nezobrazí. Ikonka bude situována v oblasti zadávání URL a při najetí kurzoru myši na ni se zobrazí stručná informace o zabezpečení. Výsledek bude vypadat přibližně takto:



Po kliknutí na ikonku klíče se zobrazí podrobnější informace o stavu zabezpečení s příslušným logem DNSSECu. Design a layout (barva okna, font, apod.) bude stejný/podobný jako v případě zobrazení detailu jakéhokoliv SSL certifikátu:



K dispozici bude také okno s možnostmi nastavení rozšíření, kde si uživatel bude moci přizpůsobit chování. Okno bude vypadat přibližně takto:

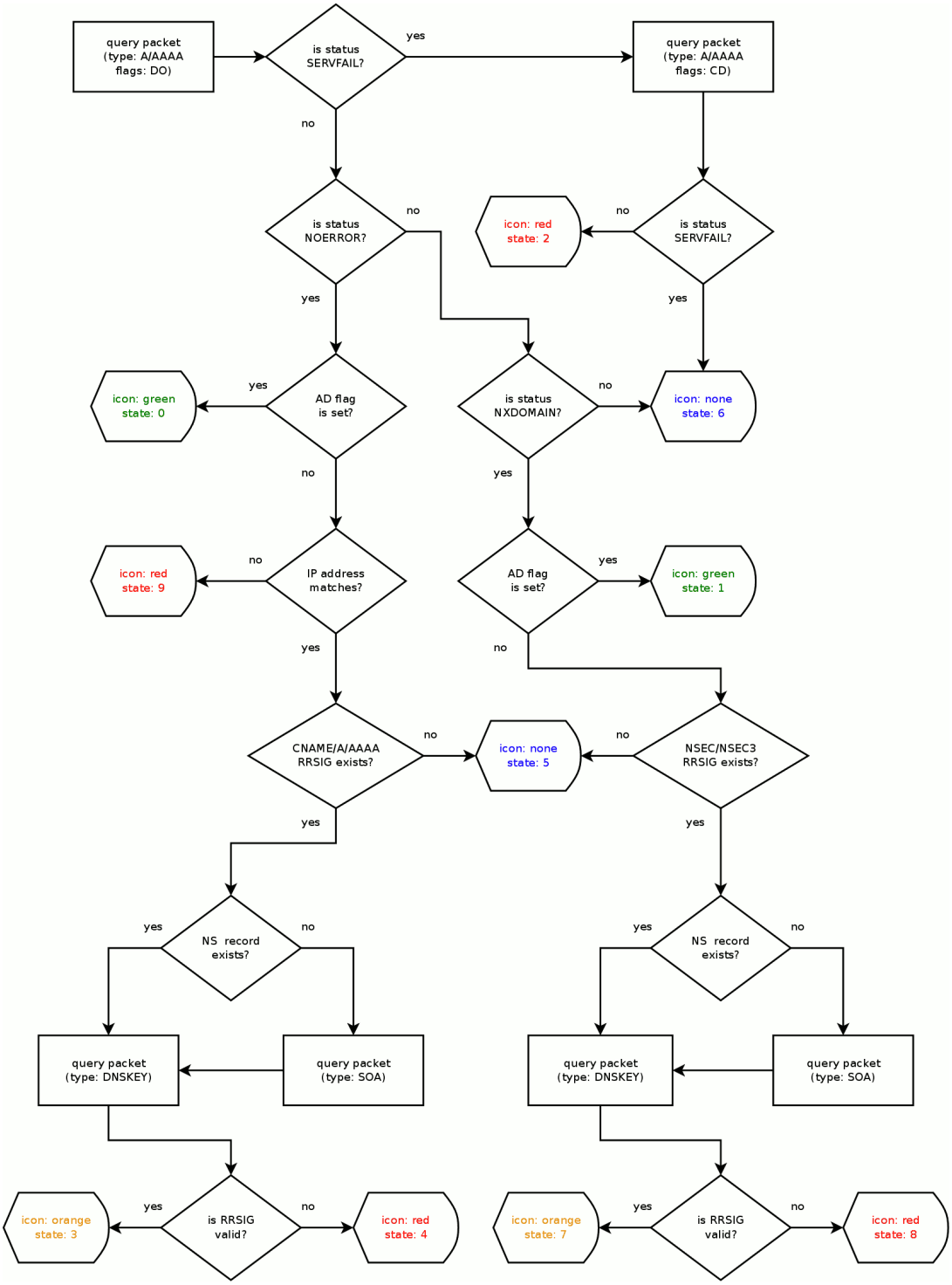


Stavový diagram

Níže uvedený stavový diagram popisuje logiku stavů rozšíření. Každý stav bude reprezentován barevnou ikonkou ve formě klíče, barevným logem s nápisem „DNSSEC“ a informačním textem specifickým pro daný stav.

Diagram pokrývá následující stavy:

- Stav 0 – doménové jméno i spojení je DNSSECem řádně zabezpečeno
- Stav 1 – spojení je DNSSECem řádně zabezpečeno, ovšem doménové jméno neexistuje
- Stav 2 – doménové jméno i spojení je zabezpečeno, ale záznam má neplatný podpis
- Stav 3 – doménové jméno má platný podpis, ovšem nelze vytvořit řetězec důvěry
- Stav 4 – nelze vytvořit řetězec důvěry, ani podpis doménového jména není platný
- Stav 5 – doménové jméno není DNSSECem zabezpečeno
- Stav 6 – stav zabezpečení je neznámý
- Stav 7 – neexistující doménové jméno je ověřeno, ovšem nelze vytvořit řetězec důvěry
- Stav 8 – nelze vytvořit řetězec důvěry, ani ověření neproběhlo úspěšně
- Stav 9 – IP adresa (adresy) rozpoznaná rozšířením pro dané doménové jméno je odišná od IP adresy (adres) rozpoznané prohlížečem



kontakt@nic.cz
www.nic.cz

Informační texty

Stav 0

Barva ikonky a loga: zelená
Nadpis: Zabezpečeno DNSSEC
Informace o doméně: Doménové jméno *www.example.cz* je zabezpečeno technologií DNSSEC.
Doplňující text: Jelikož i Váš počítač je při přístupu k vzdálenému serveru zabezpečen technologií DNSSEC, jste ochráněni proti podvržení doménového jména.

Stav 1

Barva ikonky a loga: zelená
Nadpis: Zabezpečeno DNSSEC
Informace o doméně: Neexistující doménové jméno *www.example.cz* je zabezpečeno technologií DNSSEC.
Doplňující text: Jelikož i Váš počítač je při přístupu k vzdálenému serveru zabezpečen technologií DNSSEC, jste ochráněni proti podvržení neexistujícího doménového jména.

Stav 2

Barva ikonky a loga: červená
Nadpis: Zabezpečeno DNSSEC
Informace o doméně: Doménové jméno *www.example.cz* je zabezpečeno technologií DNSSEC.
Doplňující text: Jelikož i Váš počítač je při přístupu k vzdálenému serveru zabezpečen technologií DNSSEC, byl odhalen neplatný podpis doménového jména. To může signalizovat podvržení jména útočníkem a proto nebyla cílová stránka zobrazena!

Stav 3

Barva ikonky a loga: oranžová
Nadpis: Nezabezpečeno DNSSEC
Informace o doméně: Doménové jméno *www.example.cz* je zabezpečeno technologií DNSSEC.
Doplňující text: Váš počítač ovšem při přístupu k vzdálenému serveru není zabezpečen technologií DNSSEC. Proto nelze vytvořit řetězec důvěry a může se Vám stát, že doménové jméno bude podvrženo!

Stav 4

Barva ikonky a loga: červená
Nadpis: Nezabezpečeno DNSSEC
Informace o doméně: Doménové jméno *www.example.cz* je zabezpečeno technologií DNSSEC.
Doplňující text: Váš počítač ovšem při přístupu k vzdálenému serveru není zabezpečen technologií DNSSEC, tudíž nelze vytvořit řetězec důvěry. Doménové jméno má navíc neplatný podpis, což může signalizovat podvržení jména útočníkem!

Stav 5

Barva ikonky a loga: —
Nadpis: —
Informace o doméně: —
Doplňující text: —

Stav 6

Barva ikonky a loga: —

Nadpis: —
Informace o doméně: —
Doplňující text: —

Stav 7

Barva ikonky a loga: oranžová
Nadpis: Nezabezpečeno DNSSEC
Informace o doméně: Doménové jméno *www.example.cz* je zabezpečeno technologií DNSSEC.
Doplňující text: Váš počítač ovšem při přístupu k vzdálenému serveru není zabezpečen technologií DNSSEC. Proto nelze vytvořit řetězec důvěry a může se Vám stát, že neexistující doménové jméno bude podvrženo!

Stav 8

Barva ikonky a loga: červená
Nadpis: Nezabezpečeno DNSSEC
Informace o doméně: Doménové jméno *www.example.cz* je zabezpečeno technologií DNSSEC.
Doplňující text: Váš počítač ovšem při přístupu k vzdálenému serveru není zabezpečen technologií DNSSEC. Proto nelze vytvořit řetězec důvěry a může se Vám stát, že neexistující doménové jméno bude podvrženo!

Stav 9

Barva ikonky: červená
Nadpis: Nezabezpečeno DNSSEC
Informace o doméně: Doménové jméno *www.example.cz* je pravděpodobně podvrhnuto.
Doplňující text: IP adresa vzdáleného serveru získaná prohlížečem je odlišná od IP adresy získané DNSSEC doplňkem, což pravděpodobně signalizuje podvržení doménového jména útočníkem.

Výše uvedené informační texty budou také lokalizovány do příslušných jazyků (viz sekce *Lokalizace a verze prohlížeče*).

Možnosti nastavení

Volby v grafickém nastavení rozšíření

V nastavení rozšíření budou minimálně následující položky:

- Možnost použití alternativních DNS serverů:
  - Přednastavených ODVR CZ.NICu (projekt v přípravě)
  - Přednastavených ODVR OARCu
  - Uživatelova vlastní volba
- Pro resolvování možnost použití TCP protokolu místo výchozího UDP
- Nastavení doby platnosti záznamů v mezipaměti

Skryté volby nastavitelné přes konfiguraci prohlížeče

V nastavení MF dostupném přes *about:config* půjde nastavit:

- Výpis ladicích informací na standardní výstup

Operační systémy a architektury

Projekt DNSSEC rozšíření pro MF bude realizován pro následující operační systémy:

- GNU/Linux (Debian, Ubuntu, Fedora, Gentoo, Suse), 32-bit a 64-bit intel
- Microsoft Windows (XP, Vista, 7, Server 2003, Server 2008), 32-bit intel
- Mac OS X (10.5 Leopard, 10.6 Snow Leopard), 32-bit intel a 32-bit ppc

Jelikož je prohlížeč MF v současnosti oficiálně vydáván pouze pro 32-bitové architektury, nemá prozatím smysl dělat také 64-bitové verze. Výjimkou je GNU/Linux, kde jsou již 64-bitové verze součástí některých distribucí.

Po vytvoření funkční verze pro výše uvedené platformy bude zvážena realizace i pro další systémy, např. FreeBSD. V úvahu připadá také podpora pro mobilní zařízení, především pak pro prohlížeč Fennec (mobilní verze MF). Další možností bude zvážení podpory i pro jiné prohlížeče, zejména Google Chrome, Opera a Internet Explorer.

Lokalizace a verze prohlížeče

Rozšíření bude dostupné minimálně v českém a anglickém jazyce pro prohlížeč MF verze 3.0 a vyšší.

Implementační technologie

Grafické rozhraní bude implementováno v jazycích XUL, JS, CSS. Logická část bude naprogramována v jazyce C, k níž bude přistupováno pomocí rozhraní XPCOM (C++).

Jelikož se nelze spolehnout na podporu DNSSECu systémových stub resolverů všech výše uvedených verzí operačních systémů, bude pro resolvování použita knihovna *ldns*.

Plán vývoje

Vývoj bude rozdělen do několika etap. Nejprve bude vyvinuta testovací verze pro GNU/Linux, kde bude implementováno pouze několik stavů, aby došlo k ověření vhodnosti zvolených programovacích technologií. Dále bude testovací verze portována na systémy Mac OS X a Windows, abychom ověřili použitelnost technologií i na těchto systémech. Následně bude testovací verze doplňována o další stavy a funkční části, abychom pokryli všechny možnosti dle vývojového diagramu. Jakmile dojde k „zmrazení“ vývoje, tzn. nebudou se již přidávat nové funkce, rozšíření projde důkladným testováním, aby nebyla narušena stabilita a bezpečnost prohlížeče při jeho používání. Výsledkem bude jeden instalační balíček pro MF, který bude obsahovat jak interpretovaný kód, tak všechny binární moduly včetně potřebných knihoven (ldns, apod.). Balíček bude pokud možno ke stažení z oficiální stránky doplňků pro MF, tedy z *https://addons.mozilla.org*.

Vzhledem k rozšiřující se podpoře DNSSECu přímo ve stub resolverech operačních systémů lze očekávat postupné opouštění používání ldns knihovny, zejména u OS s dostatečně odladěnou podporou. To by umožnilo zcela vypustit binární část doplňku, čímž by se podstatně zmenšila jeho velikost.

Po ukončení vývoje pro MF se předpokládá portace pro další prohlížeče, např. Google Chrome (viz sekce *Operační systémy a architektury*).

Časový harmonogram

Časový harmonogram je přibližný a bude průběžně aktualizován.

III.Q 2009 – testovací verze pro GNU/Linux, vyzkoušení zvolených technologií
IV.Q 2009 – integrace knihoven, portace na MAC OS X a Windows, kompletizace stavů
I.Q 2010 – testování, vydání stabilní verze pro MF, přechod na stub resolvery příslušných OS
II.Q 2010 – zvážení a případná realizace pro další prohlížeče