Domain Name System Security Extensions

Курсов проект по
Основи на сигурното уеб програмиране

2019/2020
летен семестър

Изготвил: Мартин Илиев, СИ 62917

Table of Contents

1. Въведение в DNS

1.1. Какво представлява DNS

Domain name system е система, която всички интернет потребители използват ежедневно, а голяма част от тях дори не подозират за съществуването и.

Различните сървари притежават собствени IP адреси, към които можем да се обърнем, за да разговаряме с тях. Това е бърза операция, която обаче притежава някои недостатъци. За повечето хора е трудно да се запомни даден IP адрес, а какво остава за запомнянето на десетки или дори стотици сайтове, които един обикновен интернет потребител знае и използва редовно. Също така, доста често се случва някои сървъри да си променят IP адреса, което допълнително ще усложни работата на хората с интернет.

Това, което DNS предоставя е възможността човек да се обръща към даден сървър с дадено име, защото за обикновения интернет потребител имената са много по-интуитивни и лесни за помнене. Например, 172.217.17.206 е доста по-сложно за запомняне от www.google.com. Накратко, когато човек напише www.google.com в браузъра си, неговата заявка бива преобразувана в заявка за IP адрес 172.217.17.206.

1.2. Как работи DNS

DNS притежава йерархия, която позволява бързо и ефективно намиране на търсения от нас адрес. Най-лесно за обяснение на въпросната йерархия е да се даде конкретен пример. Нека потребител реши да посети страницата https://learn.fmi.uni-sofia.bg. Тогава той без да си дава сметка ще мине през следните стъпки:

1.2.1 Добавяне на точка в края

Всеки символен адрес завършва с точка в края. Това означава край на името и е от голяма важност за следващите стъпки от процеса на транслиране от име в адрес.

В нашия случай това означава, че https://learn.fmi.uni-sofia.bg ще бъде трансформирано до https://learn.fmi.uni-sofia.bg. . Потребителят може спокойно да

въвежда и въпросната точка, когато иска да достъпи даден сайт, а ако не го направи, браузърът усложливо ще го направи задколисно.

1.2.2 Проверка за локален сървър

Ако операционната система поддържа собствен DNS сървър то първо ще се провери дали потребителят не се опитва да достъпи нещо в своята система. Ако не бъде намерено търсеното, системата се обръща към сървър наречен DNS resolver, който поема задачата да издири адреса на въведения сървър и да го предаде на нашата система.

1.2.3 Проверка в DNS кеш сървър

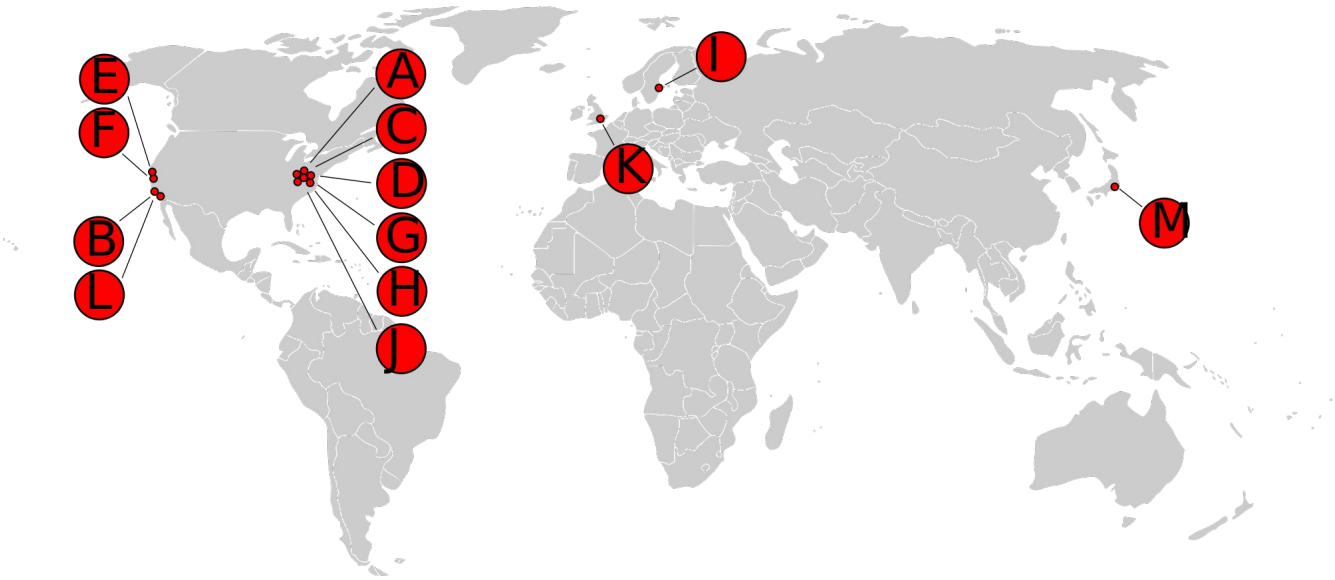
Повечето интернет доставчици поддържат DNS кеш, в който се съхраняват данните на наскоро обработените адреси. Това е първото място, където DSN resolver-а проверява.

Проверката в тези сървъри не е тежка, защото те са сравнително малки, а се указват доста ефективни. Ако търсеното име не се съдържа там се преминава към следващата стъпка.

1.2.4 Обръщане към Root nameserver

Точката, която беше добавена в 2.2.1 не е случайна както вече казахме. Тя уточнява къде е края на въпросното име и не позволява то да се третира като релативен път. Отсега нататък това, което DNS resolver-ът ще прави е да се движи наобратно по името и да разпитва различни сървъри за IP адреса, който търсим.

Първият сървър, към който се обръща resolver-ът, е така нареченият DNS root nameserver. На планета има 13 такива сървъри, които са разположени стратегически:



Тези сървъри съдържат информация за IP адресите на така наречените TLD сървъри. Както казахме, DNS resolver-ът се движи отзад напред и се опитва да намери търсеният от нас адрес, TLD е следващата стъпка от процеса. Това е частта преди последната точка, в нашия случай .bg .
Root nameserver-ът дава адреса на TLD сървъра, отговарящ за .bg на DNS resolver-а и така преминаваме към следващата стъпка.

1.2.5 Обръщане към TLD

TLD съдържа информация за всички сървъри завършващи с въпросното име. В нашия случай .bg TLD сървърът ще даде IP адреса на uni-sofia.bg, който се нарича authoritative сървър, на DNS resolver-а.

1.2.6 Обръщане към authoritative сървър

Authoritative сървърът отговаря за всички свои поддомейни, като вече става негова задача да каже на DNS resolver-а кой е адресът на learn.fmi.uni-sofia.bg. Накрая, DNS resolver-ът получава търсеният адрес ако въобще съществува.

1.2.7 DNS resolver-ът предава адреса на потребителя

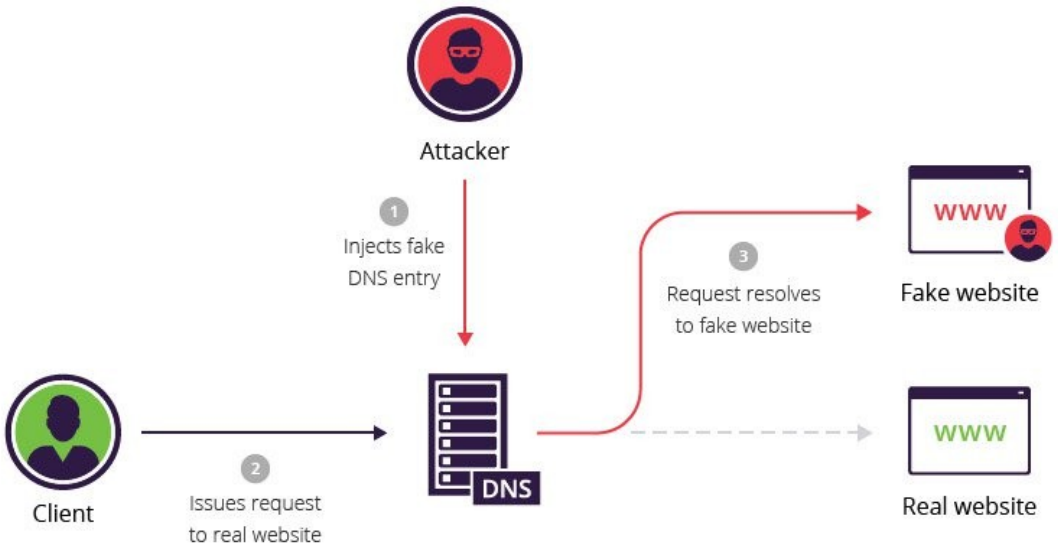
Накрая потребителят получава търсеният от него адрес и може да се свърже към него.
Макар да изглежда бавна и тромава, тази процедура се случва за части от секундата и благодарение на нея интернет е това, което познаваме днес.

2. DNS фишинг

2.1 Какво представлява фишинг

Сериозен риск за сигурността в работата на DNS е фактът, че данните, които се обменят между различните сървъри, са в обикновен текст. Това прави много лесно за някой Man in the middle да разбере какво търсим и да манипулира резултата. Ако резултатът бъде манипулиран то потребителят ще получи някакъв друг IP адрес и ще отиде там, като естествено това само по себе си е огромен риск.

Това, което е по-страшно от просто една заявка към грешен IP адрес е кеширането. Както беше отбелязано в точка 1.2.3, наскоро достъпваните сайтове се съхраняват в cache сървъри от интернет доставчика. По този начин въпросният Man in the middle може да навреди и на други хора използващи същия интернет доставчик. Тази атака се нарича фишинг или отравяне на кеша.



2.2 Възможни щети нанесени от фишинг

След като DNS отговорът бъде манипулиран, хакерът може да препрати потребителя към специално пригоден за фишинг адрес, изцяло под негов контрол. Обикновено тези сайтове много приличат на оригиналните, макар да нямат тяхното DNS име, цялостен вид и най-важното SSL/TLS сертификат.

Въпреки тези си недостатъци, голяма част от потребителите не обръщат внимание на тези детайли, а сляпо се доверяват на DNS resolver-а. След това те могат да започнат директно да свалят файлове от този доверен сайт и още по-лошото да ги инсталират, което обикновено води до заразяване на локалната машина с вирус. Възможно е и да бъдат пренасочени до http сървър, където усложливо да си въведат личните данни, които злонамереното лице да извлече и после да приложи в истинския сайт (например банков акаунт).

Този тип атаки разчита на доверието, което потребителите са натрупали с годините към работата на DNS и тяхната небрежност спрямо опасностите, които се крият в интернет. Затова потребителят трябва винаги да проверява за наличието на иконка за валиден сертификат на сайта, както и да следи на кой url се намира особено, когато е на път да въвежда лични данни.

3. Domain Name System Security Extensions

3.1 Създаване на метод за борба с подмяната на отговор от DNS

Отговорната за DNS протокола организация Engineers in the Internet Engineering Task Force (IETF) бързо осъзнава опасността описана в точка 2 както и някои други рискове в системата причинени от липсата на автентикация на отговора предоставен на DNS resolver-а. След години работа тяхното решение на проблема е Domain Name System Security Extensions (DNSSEC).

3.2 Какво предоставя DNSSEC

Това, което DNSSEC предоставя е:

- Валидиране, че източникът на данните е този, към когото сме направили запитване
- Валидиране на данните са неподправени и пълни
- Защита на потребителя и целия кеш сървър на интернет доставчика от фишинг

Това, което DNSSEC не предоставя е:

- Криптиране на данните и скриване на нашата онлайн активност
- Защита на заявката ни от атака по пътя (заявката може да бъде компроментирана, но тогава ще сме защитени от последиците)

- Гаранция че, сайта който посещаваме е сигурен и има нужните сертификати

3.3 Начин на работа на DNSSEC

3.3.1 Дигитален подпис от собственика на зоната

Основната концепция на DNSSEC е използването на криптографски ключове (публичен и личен). Накратко, това е криптографски алгоритъм, който има 2 ключа, които са специално избрани така, че единият да криптира информацията по такъв начин, че само другият ключ да може да я декриптира.

Единият ключ е публичен и се разпространява свободно, а другият ключ е личен и не се споделя с абсолютно никого. Така се гарантира, че ако някой в интернет иска да контактува с конкретен сървър, то информацията помежду им се предава сигурно, защото е почти невъзможно някой да успее да я подправи заради сложността на криптографския алгоритъм.

Идеята за дигитален подпис е изцяло базирана на този принцип. За да се валидира, че изпратеното съобщение в чист текст е истинно, подателят го криптира и предоставя и криптираната версия на текста. Така получателят може да декриптира получената версия и да верифицира, че съобщението в обикновен текст е истинно.

Използвайки този принцип, в DNSSEC, собственикът на зоната връща на DNS resolver-а не само изисканите от него данни, но и криптираната им форма чрез неговия личен ключ. Собственикът на зоната е предоставил публичния си ключ и лесно може да се валидира от DNS resolver-а дали получените данни са истинни или подправени.

3.3.2 Автентичност на предоставения публичен ключ за автентициране на получения дигитален подпис

Описаната в точка 3.3.1 процедура изглежда добре, но има някои неща, които изглеждат като потенциален риск. Например, възможно е злонамереното лице реши да подаде грешни данни, които да криптира с негов личен ключ и да предостави публичния ключ за неговия личен ключ. Тогава цялата идея за DNSSEC се обезсмисля и проблемът в точка 2 остава нерешен като единственото, което се постига с DNSSEC е по-бавен интернет достъп.

Решението за валидиране на публичния ключ, предоставен от собственика на зоната, е той също да бъде криптиран, но този път с публичния ключ, предоставен от предходния DNS сървър. Ако вземем за пример сайта learn.fmi.uni-sofia.bg от точка 1.2 то ние сме получили неговия IP адрес от authoritative сървъра uni-sofia.bg. Ако този сайт поддържа DNSSEC той ще ни предостави публичния си ключ с дигитален подпис не от него, а от TLD сървъра .bg. След това ние ще можем да се обърнем към TLD сървъра, който да потвърди, че това наистина е публичния ключ на uni-sofia.bg.

Това обаче реално не решава проблема с подменен ключ, защото може и публичния ключ на .bg да е бил подменен. И отново се връщаме в началото. Решението на този проблем е същото като в горния параграф. Публичният ключ на TLD сървъра е с дигиталния подпис на неговия предшественик – root сървъра.

Така се указва, че публичните ключове на всяка зона са подписани от техните предшественици и накрая стигаме до root server-a, който няма предшественици, които да подпишат ключа му. Това все още не решава проблема с подменени ключове, но реално това ограничава броя на сървъри излагащи на опасност DNS до 13, което е много по-малко от няколко милиарда. Остава да се направи така, че да може да се валидира, че ключът предоставен от root.

Решението на този проблем е да има ключове, които са проверени и внедрени в системата по подразбиране. Такъв ключ например е този за root сървърите. Тъй като те са малък брой е много лесно да бъдат въведени в системата по подразбиране. Повечето браузъри също разполагат с такива ключове по подразбиране. Тези ключове са много добре пазени на локално ниво и подмяната им е възможна само ако злонамереното лице придобие цялостен достъп до самата ни система, което само по себе си застрашава всичко в самата система.

Цялата процедура по криптирането на ключове с други ключове се нарича верига на доверие (chain of trust). Първоначалният ключ, който е в началото на системата се нарича „котва на доверие“ (anchor of trust). Той е потвърден по подразбиране и системата му вярва сляпо. На базата на това доверие, се изгражда цялата верига от доверие, където всеки следващ ключ във веригата е криптиран с предхождащия го.

По този начин вече злонамереното лице не може да измами потребитекля освен ако не подмени добре пазената котва.

3.3.3 Работа на DNSSEC при несъществуваща цел

Ако потребител се опита да достъпи сървър, който не съществува чрез DNS той получава празен отговор, който всеки браузър интерпретира различно (обикновено чрез съобщение за ненамерен сървър или търсене в някой search engine).

Празното съобщение обаче е проблем за DNSSEC, защото няма какво да се криптира. За да се справи с това, DNSSEC добавя NSEC и NSEC3 записи. Най-общо казано те позволяват автентицирано отричане на съществуване (authenticated denial of existence).

Това създава известно неудобство в работата на DNSSEC и е източник на потенциални рискове в системата, които са описани в точка 6.2

3.3.4 Алгоритми, използвани за криптиране в DNSSEC

DNSSEC е измислен така, че да може ако някой от използваните криптиращи алгоритми бъде разбит по някакъв начин той да бъде заменен с друг. Следната таблица дефинира алгоритмите, които най-често се използват в DNSSEC от април 2013:

Поле на алгоритъм	Алгоритъм	Източник	Статус на имплементация
1	RSA/MD5		Не бива да се имплементира
3	DSA/SHA-1		По желание
5	RSA/SHA-1	RFC 3110	Задължително

7	RSASHA1-NSEC3-SHA1	RFC 5155	Препоръчително
8	RSA/SHA-256	RFC 5702	Препоръчително
10	RSA/SHA-512		Препоръчително
12	GOST R 34.10-2001	RFC 5933	По желание
13	ECDSA/SHA-256	RFC 6605	Препоръчително
14	ECDSA/SHA-384		Препоръчително
15	Ed25519	RFC 8080	По желание
16	Ed448		По желание

Digest field	Digest	Source	Implementation status[8]
1	SHA-1	RFC 3658	Задължително
2	SHA-256	RFC 4509	Задължително
3	GOST R 34.10-2001	RFC 5933	По желание

4	SHA-384	RFC 6605	По желание

3.4 Поддръжка на DNSSEC

Следната таблица представя поддръжката на DNSSEC от големите оператори:

Регистър (домейн на authoritative сървър)	Брой домейни	Брой домейни с DNSSEC key	DNSSEC поддръжка от регистър	DNSSEC поддръжка от собственик
GoDaddy (domaincontrol.com)	37,652,477	8,139	ДА	ДА
Alibaba (hichina.com)	4,292,138	3	НЕ	НЕ
1AND1 (1and1)	3,802,824	0	НЕ	НЕ
Network Solution (worldnic.com)	2,534,673	0	НЕ	НЕ
eNom (name-services.com)	2,525,828	10	НЕ	ДА
Bluehost (bluehost.com)	2,066,503	0	НЕ	НЕ
NameCheap (registrar-servers.com)	1,963,717	13,232	Само за някои планове	ДА
WIX (wixdns.net)	1,887,139	0	НЕ	НЕ
HostGator (hostgator.com)	1,849,735	0	НЕ	ДА
NameBright (namebrightdns.com)	1,823,823	0	НЕ	ДА
register.com (register.com)	1,311,969	0	НЕ	НЕ
OVH (ovh.net)	1,228,578	319,580	ДА	ДА
DreamHost (dreamhost.com)	1,117,902	0	НЕ	ДА
WordPress (wordpress.com)	888,174	3	НЕ	НЕ
Amazon (aws-dns)	865,065	0	НЕ	ДА

Xinnet (xincache.com)	836,293	0	НЕ	НЕ
Google (googledomains.com)	813,945	1.945	НЕ	ДА
123-reg (123-reg.co.uk)	720,435	1	НЕ	ДА
Yahoo (yahoo.com)	690,823	0	НЕ	НЕ
Rightside (name.com)	663,616	0	НЕ	ДА

3.5 Популярност на DNSSEC

Голяма недостатък на DNSSEC е, че се използва на много малък процент от сървърите. Една от причините е липсата на поддръжка от големите регистри.

От 20-те най-популярни регистри, които държат ~ 54.3% от .com, .net и .org домейните, само 3 поддържат DNSSEC. Това означава, че техните потребители няма да могат да използват DNSSEC на техните сървъри ако използват nameserver-ите на регистъра. Все пак 11 от сървърите позволяват да се използва DNSSEC ако потребителят използва външен nameserver, но това е доста голямо неудобство.

Съществуват различни кампании за насърчаване на използване на DNSSEC, но за момента те не са много успешни и все още тази технология не се е наложила глобално.

4. Внедряване на DNSSEC

4.1 Предизвикателства пред налагането на DNSSEC

Както вече беше споменато, DNS е гръбнакът на съвременния интернет и без него интернет не би могъл да достигне сегашното си ниво на популярност, както и че DNS е изключително незащитен и податлив на злонамерени атаки, които могат да имат сериозни последствия при невнимание на потребителя. Тези проблеми не са обществена тайна като както хората отговорни за DNS са ги признали. Също така доклада за национална стратегия за киберсигурност на САЩ посочва нуждата за защита на DNS. Смята се, че внедряването на DNSSEC мащабно би разрешило идруги проблеми, като незащитеността при обмяна на ключове за имейли.

Самото внедряване на DNSSEC в големи мащаби обаче има много предизвикателства, с които трябва да се справи. Една от най-големите пречки е, че потребителите обикновено само внедряват технологии ако ще получат моментално облагодетелстване от това, а не ако се очаква в бъдеще това да укаже влияние. За да бъде DNSSEC наистина ефективен, трябва да се използва глобално, а не в такава малка част от сървърите както е в момента.

Също беше споменато и за един от недостатъците на DNSSEC – нуждата от време, което може да е доста неприятно за крайния потребител особено при по-слаба интернет връзка. Една от причините за това е, че повечето DNSSEC отговори са по-леми от типичните 512 байта за UDP. Този проблем може да се реши чрез фрагментиране на данните, но това води до други проблеми. Така се стига до нуждата от употреба на TCP, което сигурно, но е и бавно.

4.2 Ранно внедряване

Едни от първите внедрили DNSSEC са Бразилия (.br) , България (.bg) . Чехия (.cz), Намибия (.na), Пурто Рико (.pr) и Швеция (.se), които използват DNSSEC за техните национални TLD сървъри. През февруари 2007, датската компания TDC A/S става първият интернет доставчик в Швеция, който предлага тази технология на клиентите си.

През юни 2007, IANA публично тества примерен подписан root сървър. На 23-ти юни 2010, 13 регистъра са обявени за предлагащи DNSSEC услугата за .org домейни.

4.3 Внедряване на DNSSEC в DNS root сървър

DNSSEC за първи път е внедрен в root сървър на 15-ти юли 2010. Това е ключово, защото наличието на DNSSEC в root сървър позволява споменатата в точка 3.3.2 котва.

4.3.1 Технически проблеми

Това обаче не е цялостно решение на въпроса с веригата на доверие. Ако някоя от зоните в адреса не е потвърдена като безопасна, то се налага създаването на нова котва. Например, ако зоната "signed.example.org" е сигурна, но зоната

"example.org" не е, макар “.org” и root да са сигурни, то пак се налага внедряването на допълнителна котва, която да валидира зоната.

4.3.2 Политически проблеми

Някои държави са притеснени по политически подбуди за подписането на root сървъра, защото контролът на САЩ над интернет става твърде голям и по тази причина отказват централизирането на ключове. Някои правителства дори забраняват разпространението на DNSSEC-backed ключове.

4.3.3 Планиране

На 3-ти юни 2009, Националният исктитут по стандарти и технология (NIST) обявява планове да подпише root сървърите до края на 2009 в съвместна работа с ICANN, VeriSign and the NTIA.
На 6-ти октомври 2009, ICANN и VeriSign обявяват плана за постепенно подписане на root сървърите, което се очаква да започне на 1-ви декември 2009 и в продължение на 13 месеца да се подписва по един root сървър.

4.3.4 Изпълнение

Процедурата минава по-добре от планираното, като на 15-ти юли 2010 всички root сървъри са подписани, като root котвите могат да бъдат изтеглени от IANA.org.

4.4 Внедряване на DNSSEC в TLD сървърите

За разлика от root сървърите, където постигането на пълно поддържане на DNSSEC е лесно постижимо, при TLD има много сървъри, в които DNSSEC трябва да се внедри, а това не се случва по различни политически причини. Още на това ниво идеята за цялостна поддръжка на DNSSEC пропада и става невъзможно на долните нива да се стигне до цялостна поддръжка.

Тъй като става дума за много сървъри, този линк може да даде информация на читателя за TLD сървърите, които не поддържат DNSSEC: линк

5. Добавяне на DNSSEC защита към домейн

5.1 Предварителни изисквания

5.1.1 TLD сървъра на домейна трябва да е подписан

Както беше споменато в точка 4.4, не всички TLD сървъри поддържат DNSSEC, което е една от основните прични DNSSEC да не може да постигне пълно покритие. Затова първото, което трябва да се провери преди захващане с добавяне на DNSSEC към даден домейн е дали това е възможно да се случи за този TLD.

5.1.2 Регистраторът на домейна трябва да поддържа DNSSEC

Регистраторът, където е бил регистриран въпросният сайт трябва да поддържа DNSSEC. Най-вече трябва да може да приема и подписва Delegation Signer (DS) записи, които съдържат нужната информация за използваните ключове за подписване на DNS зоната.

На този линк може да се проверят всички регистратори, които поддържат DNSSEC: линк

5.1.3 DNS hosting доставчика на домейна трябва да поддържа DNSSEC

Много често се случва регистраторът на домейна да предлага и DNS hosting. Възможно е обаче за DNS hosting да се използва друга фирма или самият собственик на сайта да си е host. Без значение кой е DNS hosting доставчик, той трябва да поддържа DNS. Повечето доставчици се стремят да автоматизират тази услуга с цел да улеснят потребителите си и затова процедурата за добавяне на DNSSEC към домейна е различна за различните доставчици, като повечето от тях предлагат детайлно описание как може да се получи услугата.

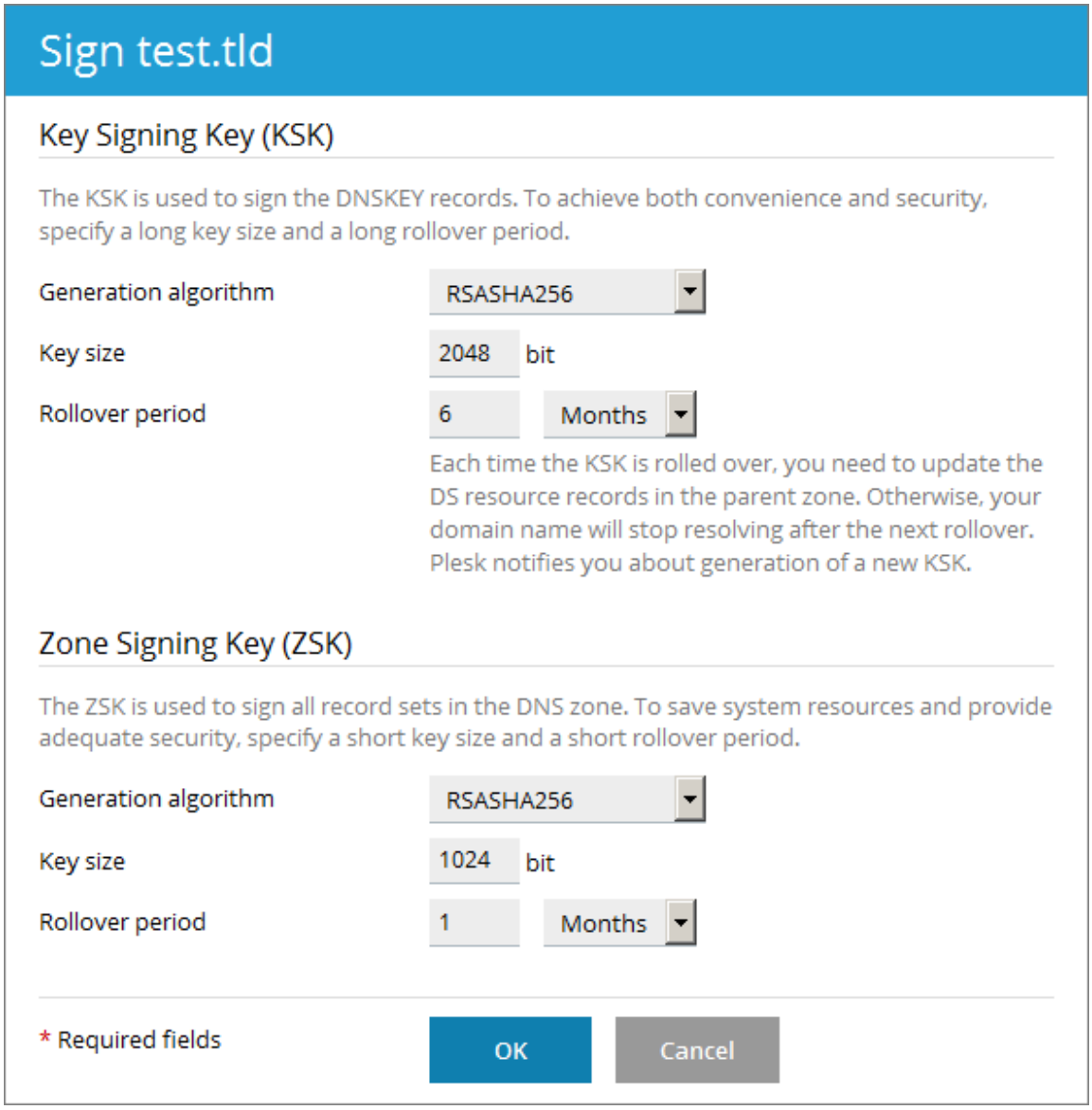
5.2 Добавяне на DNSSEC към домейн

*Тъй като за всеки хостинг доставчик този процес е различен, а е добре да се даде реален пример, ще се покаже как се добавя DNSSEC към домейн, поддържан от plesk.

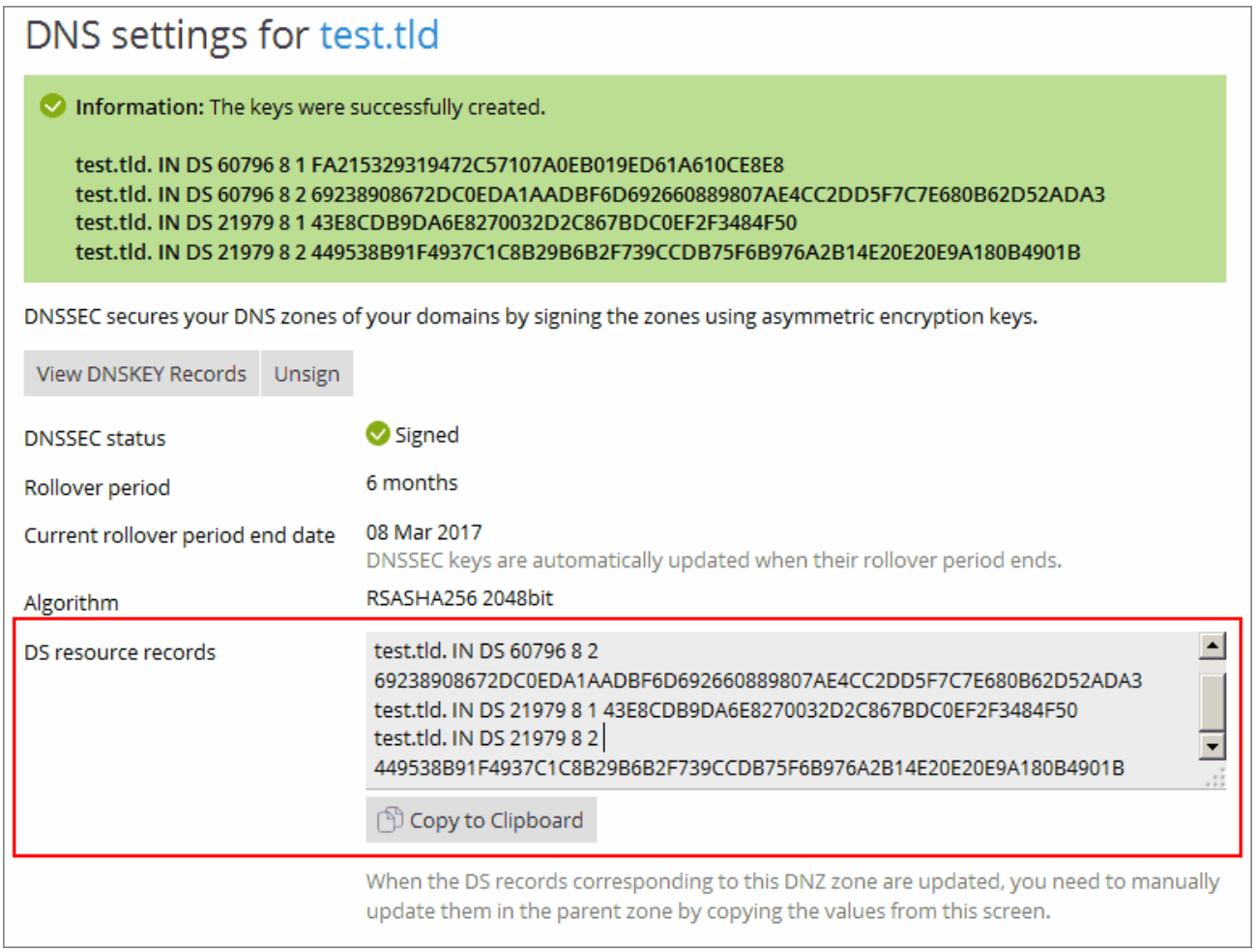
Plesk автоматично генерират нужните ключове – за подпис на зоната и за подпис на самия ключ. Също така Plesk предоставят и удобен GUI за потребители, които

не се чувстват комфортно без такава среда. Следващите стъпки се случват именно в графична среда на техния сайт.

1. Отиване на страница Websites & Domains
2. Отиване на DNSSEC и кликане върху Sign the DNS Zone
3. Избиране на алгоритмите за криптиране, чрез които да се създаде ключът:



4. След като приключи подписването, Plesk показват DS записи, които съдържат хешове на ключовете за подписване на зоната. Тези данни трябва да се копират и да се поставят в родителската зона на домейна:



5. Вече домейнът е защитен с DNSSEC

6. Слабости в системата на DNSSEC + DEMO??? (5 стр.)

6.1 Недостатъчно разпространение

DNS фишингът е много опасна атака, но в същото време е и трудна за изпълнение, а дори да е успешна е много вероятно да се провали ако потребителят е невнимателен. DNSSEC забавя една от най-критичните операции в интернет, изисква много работа за правилна поддържка и често пъти създава неудобство на администраторите на зоната, а единственото, което предлага в замяна, е защита срещу една доста рядка атака.

Поради изброените по-горе причини, много хора не искат да се занимават с DNSSEC и поемат риска клиентите им да може да бъдат незащитени от фишинг атаки. Заради това DNSSEC не се използва глобално и по този начин неговата сила намалява. Това затруднява развитието на технологията, тъй като е по-трудно да се наблюдава функционирането на технологията, хакерите не се борят достатъчно

срещу него и е трудно да се подобри защитата му, което означава, че крие потенциални пробиви в защитата, които може да бъдат открити прекалено късно.

6.2 Обхождане на зоните чрез DNSSEC NSEC

NSEC се използва за автентициране на несъществуващ DNS запис. Това предоставя възможност на злонамереното лице да преброи всичките имена в една зона като следва NSEC веригата.

NSEC проверява дали името съществува в дадена зона като свързва от съществуващо име към съществуващо име заедно с каноничното подреждане на всички имена в зоната. Атакуващият може да провери тази последователност и да получи всичките имена в зоната в хеширана форма. Това позволява да се разбере броя на имената в зоната, но не и кои са те, но рядко в хешированието се използва достатъчно добра сол и особено кратките имена са много податливи на разбиване чрез използването на brute-force методи.

6.3 Замяна на ключове

С течение на времето нараства рискът използваният ключ да бъде компроментиран по някакъв начин (небрежност, криптоанализ или пък някаква нова уязвимост в системата за криптиране). Това налага замяната на ключовете с нова двойка.

По време на замяната на ключове , публикуваните данни за предишната двойка остават в някои кешове. Ако тези данни бъдат игнорирани може да се стигне до загуба на услуги за клиенти, особено когато resolver, който не пази кеширан стария ключ се опитва да валидира данни от зона, подписана със стария ключ. Всъщност ако старият ключ вече не присъства в зоната, цялата операция се проваля и DNSSEC третира това като опит за фишинг.

Също така замяната на ключа на root сървър е трудно постижима, защото засега цялата йерархична база от данни. Процесът на пълна замяна на ключа на root сървър отнема години поради факта, че трябва да се ъпдейтнат всички сървъри включително и личните компютри на хората, а има такива, които рядко се свързват към интернет и ако замяната се случи без те да са ъпдейтнали може да е невъзможно за тях да използват множество интернет услуги.

6.4 Офлайн съхранение на личен ключ

Препоръчително е личния клюя да се съхранява офлайн. Това създава проблеми с поддържката на динамични ъпдейти, тъй като тогава ключът не може да се използва за подписване в реално време с цел автентициране на динамично ъпдейтнати данни.

Това прави динамичното ъпдейтване на данни в DNSSEC или неналично, или незащитено, защото пробив в сигурността на сървър, който съдържа личния си ключ, може да предостави на злонамереното лице пълен достъп до зоната. Заради това се препоръчва ключът да не бъде онлайн, макар това да е за сметка на динамични ъпдейти.

6.5 DNSSEC проблеми с времето

DNSSEC се нуждае от време за синхронизация между resolver-а и host-а, който генерира DNSSEC подписа. Resolver-ът трябва да има същата концепция за абсолютно време с цел да определи дали подписът е валиден или изтекъл.

Злонамерено лице може да промени възприятието за абсолютно време на resolver-а с цел да го накара да използва изтекъл подпис. Също така злонамерено лице може да промени ъзприятието за абсолютно време на собственика на зоната с цел да го накара да създаде подпис с различен период на валидност.

Подписите не се генерират за всяко поискване, а се запазват след генериране за доста време - голям Time to Live (TTL), защото подписването е скъпа операция откъм време. Това отваря възможности за различни атаки, където вече остаряла информация се предава отново на потребителя и тъй като подписът все още не е изтекъл всичко изглежда наред. По този начин смяната на подпис се указва неефективна докато не изтече големия TTL и затова трябва да се внимава много през този период именно за такива атаки.

6.6 По-голямо време за изчисления

DNSSEC значително увеличава размера на DNS пакетите, което драстично увеличава изчисленията, които DNS сървърите трябва да правят и увеличава нужното време за отговор. Процесът по верифициране на подписаните записи сам по себе си изисква доста изчислителни ресурси, особено за по-големи ключове.

DNSSEC стандартът позволява до 1024-битови ключове. Добавяйки дигитален подпис към домейн увеличава всеки запис ~ 5-7 пъти, което е голямо натоварване за сървърите, DNSSEC отговорът увеличава натовареността на resolver-a, тъй като поддържащите DNSSEC resolver-и ще трябва да изпълнят валидация на подписи, а в някои случаи ще трябва да се занимават и с допълнителни заявки. Това претоварване ще увеличи нужното време за отговор към машината направила първоначалното запитване.

6.7 Малък брой инструменти за управление

DNSSEC е значително по-сложен от DNS. В момента има много малък брой базови инструменти за улеснение на процеса по подписване. Все още няма готови инструменти за следене и анализ на логове. Ръчното дебъгване не много трудно и изисква много време

6.8 Липса на системен контрол

DNSSEC използва проста схема за репликиране чрез главен и вторичен name сървър, за да предостави по-голяма наличност на сървъра и да подобри разпределението на натовареността. Само един от двата сървъра взима участие в конкретна заявка, защото един компроментиран клиентски сървър е достатъчен да блокира, открадне или пренасочи информация.

Ъпдейтването на данни се случва само в главния name сървър и вторичния не е наясно за новостите от ъпдейта докато не се случи следващия zone transfer. По този начин, може да се получи неконсистентност между състоянията на двата name сървъраи една заяква от клиентски сървър може да получи два напълно различни резултата в зависимост от това през кой сървър е минал. Това причинява проблеми с консистентността и надеждността дори без умишлена външна атака.

6.9 DNSSEC проблеми възникнали в .NL

SEGREG е DNSSEC експеримент проведен от NLNetLabs. По време на експеримента един от .nl вторичнтите домейни (dnssec.nic-se.se) не се ъпдейтва в продължение на две седмици заради преливане на паметта. Това причинява огромни проблеми, защото валидността на един подпис за .nl е една седмица и по този начин подписите на dnssec.nic-se.se изтичат. Заявките на потребителите на

сървъра се указват невалидни за .nl , а още по-лошото е, че при DNSSEC вторични домейтни, които имат изтекли подписи, биват премахнати локално от домейна.

6.10 Твърдения, че DNSSEC увеличава риска от наводнение на сървъра

В различни източници се твърди, че DNSSEC е опасност за сървъра, защото EDNS0 разширението на съобщенията подпомага DDoS атаките, защото допълнително забавя цялата система. Макар да изглежда правдоподобно, това не е вярно.

DNSSEC наистина задължително трябва да използва EDNS0, но EDNS0 може да се използва и без DNSSEC и реално се използва и от други различни от DNSSEC отговори, които са толкова големи колкото и DNSSEC. Такива отговори например са TXT записите, които се използват за представяне на SPF политики или DKIM ключове. Също така някои множества от MX записи са огромни и без да използват EDNS0.

Така се указва, че DDoS атаките не разчитат особено на DNSSEC, защото има и много други записи, които могат да изполват. DNSSEC има много проблеми, но опасенията, че при DDoS атака сървърът ще се разпадне заради него са силно преувеличени и дори неверни.

7. Заключение

DNS е система, без която човечеството не може да продължи да използва интернет. Като нещо толкова важно, тя трябва да бъде защитена от всякакви възможни злонамерени действия.

В действителност, обаче, DNS притежава множество проблеми със сигурността, които трябва да се адресират незабавно. Заплахи като Man in the Middle и отравяне на cache се появяват заради липса на автентикация и цялостност в DNS процеса. Възможни са и неволни грешки в употребата на DNS като грешно конфигурирани resolver сървъри или филтри за пакети, които създават ситуация подобна на DDoS атака.

Internet Engineering Task Force (IETF) създава DNSSEC в отговор на проблеми за цялостност и фишинг. Това е сигурен DNS протокол, който позволява автентикация по време на самото търсене на ip адреса и по този начин защитава и самите зони по време на процеса.

DNSSEC не предпазва от препълване на буфери или от DDoS атаки както и не предоставя конфеденциалност. DNSSEC зоновите файлове са значително по-големи от техните DNS алтернативи, като и се изискват повече ресурси за обработката им.

Публичните и личните ключове може да се компроментират с времето. Ключовете трябва да се сменят периодично, за да се намали риска това да се случи, Тази процедура може да се постигне сравнително лесно на по-долните нива от DNSSEC йерархията, тъй като публичните ключове не се кешират за дълго време. Нещата обаче не стоят така за root сървърите, защото цялата верига на доверие е базирана на факта, че се знае със сигурност кой е root ключа.

По-голямата част от интернет доставчиците и регистраторите не одобряват DNSSEC и смятат, че без него е по-добре, защото работата с него е сложна и значително намалява бързодействието на DNS, което прави техните услуги по-нискокачествени. Те смятат, че ползите, които носи употребата на DNSSEC, са по-малко от неудобството, което създава, и затова не го поддържат.

Въпреки посочените слабости в точка 6, DNSSEC наистина предоставя автентициране и цялостност на DNS данните. В момента технологията се намира в застой, породен най-вече от нежеланието на много компании да го предлагат и използват.

Възможно е в бъдеще да се появи друга алтернатива на DNSSEC, която да не притежава споменатите недостатъци и да изпълнява същите функции. Друга възможност е да се отстранят проблемите в DNSSEC по някакъв начин като, например, да се открие по-бърз алгоритъм за криптиране, който да не забавя толкова процеса.

Само бъдещето може да отговори на тези въпроси. Това, което е ясно в момента, е, че DNS технологията има пропуски в сигурността и най-доброто решение, което

имаме в момента за тях, може да ги реши напълно, но на твърде висока цена, която повечето предприемачи не са готови да платят.

8. Източници

https://cloudacademy.com/blog/how-dns-works/ - точка 1.2
https://upload.wikimedia.org/wikipedia/commons/thumb/5/5e/Root-historic.svg/2000px-Root-historic.svg.png – точка 1.2.4
https://en.wikipedia.org/wiki/DNS_spoofing – точка 2
https://www.imperva.com/learn/wp-content/uploads/sites/13/2019/01/DNS-spoofing.jpg – точка 2.1
https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en – точки 3.1 и 3.2
https://www.cloudflare.com/dns/dnssec/how-dnssec-works/ - точка 3.3
https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions – точки 3.3.4 и 4.
https://blog.apnic.net/2017/12/06/dnssec-deployment-remains-low/ -точка 3.4
https://www.internetsociety.org/deploy360/dnssec/registrars/ - точка 5.1
https://docs.plesk.com/en-US/onyx/customer-guide/websites-and-domains/domains-and-dns/configuring-dnssec-for-a-domain.76433/ - точка 5.2
https://serverfault.com/questions/708076/what-kinds-of-security-vulnerabilities-does-providing-dnssec-expose/747213 – точки 6.1 и 6.10
https://www.researchgate.net/publication/221548408_Security_vulnerabilities_in_DNS_and_DNSSEC – точки 6.2-6.9 и 7