آسیب پذیری های امنیتی در DNS (سیستم نام دامنه) و DNSSEC (توسعه امنیت سیستم نام دامنه)

کاظم فریدی[۱]،زینب مرادیان[۲]
[۱]کارشناسی ارشد، دانشکده فنی مهندسی دانشگاه آزاد اسلامی واحد بافت ، kazem.faridi@iaubaft.ac.ir
[۲ ۱]کارشناسی ارشد، دانشکده فنی مهندسی دانشگاه آزاد اسلامی واحد بافت ، zynabmoradyann@yahoo.com

چکیده:

داده های سیستم نام دامنه (DNS) که توسط سرورهای نامگذاری ایجاد می گردند فاقد پشتیبانی تایید منشاء داده و یکپارچگی داده ها می باشند. این فرایند، سیستم نام دامنه (DNS) را در معرض حمله کاربران (MITM) و همچنین مجموعه ای از حملات دیگر قرار می دهد. برای اینکه سیستم نام دامنه (DNS) قدرتمند تر شود، DNSSEC ، توسط کمیته کارگروه مهندسی اینترنتی (IETF) مطرح شده است. DNSSEC مجوز منشاء داده و یکپارچگی داده ها را با استفاده از علائم دیجیتالی ایجاد می کند. اگرچه DNSSEC ،امنیتی را برای داده های سیستم نام دامنه (DNS)ایجاد می کند، از نقص های جدی عملیاتی و امنیتی زیان می بیند. ما به بررسی طرح های DNS و DNSSEC پرداخته، و آسیب پذیری امنیتی مربوط به آن ها را مد نظر قرار می دهیم.

واژه های کلیدی:

سیستم نام دامنه ، توسعه امنیت سیستم نام دامنه،پروتکل اینترنتی،ایستگاه پردازش،سرور و کلاینت

۱- مقدمه

DNS به عنوان یک مکانیسم استاندارد برای نامگذاری مجزای آدرس IP (پروتکل اینترنتی) می باشد. به دلایل امنیتی و قابلیت دسترسی این مسئله حائز اهمیت می باشد که DNS قادر به تحمل نقص ها و حملات باشد. این موارد از حملات اخیر گسترده که با آلوده کردن حافظه نهان DNS اطلاعات مالی حساس را سرقت کرده است، مشخص می گردد.

برای بر طرف کردن مشکلات امنیتی شناخته شده با DNS، مجموعه ای از موارد توسعه یافته امنیتی مطرح شده است. DNSSEC منجر به یکپارچگی داده ها و تایید منشاء آن ها با استفاده از علائم دیجیتالی از پیش ساخته برای هر داده که در پایگاه داده DNS ذخیره می شوند، می گردد. به هر حال همان طور که ما در این مقاله نشان می دهیم، DNSSEC به معرفی موضوعات امنیتی جدید همانند زنجیره ای از موضوعات مربوط به اعتماد، و حملات همزمان و زمان بندی شده، عدم پذیرش تقویت سیستم، افزایش ظرفیت محاسبه، و دامنه موضوعات مدیریت کلیدی می پردازد.

DNS نام دامنه ها را به آدرس IP، و بلعکس تبدیل می کند. DNS به عنوان یک پایگاه داده توزیع شده جهانی بوده که از ساختارهای زنجیره ای پشتیبانی می کند. شناسه کلاینت که به عنوان یک تصمیم گیرنده شناخته می شود به عنوان یک کلاینت (ایستگاه پردازش) جستجو را انجام داده و پاسخی را از سرور DNS دریافت می کند. این پاسخ ها شامل موارد ثبت شده منابع (RRS) و حاوی اطلاعات تفکیک شده نام/ آدرس مورد نظر می باشد. دسترس پذیری و عملکرد DNS از طریق مکانیسم تکرار و ذخیره سازی بالاتر می رود. شرح مفصل عملکرد DNS در بسیاری از کتاب ها وجود دارد.

بخش نامگذاری DNS به صورت زنجیره ای سازماندهی می گردد. دامنه به عنوان زیرشاخه بخش نامگذاری می باشد. دامنه هایی که بیشتر مورد استفاده قرار می گیرند (TDLs) همان هایی هستند که در زیر ریشه قرار می گیرند. دامنه ی که به واحدهای کوچکتری تقسیم می شود به نام ناحیه دسته بندی می باشد.

۲- سرور های نامگذاری و تصمیم گیرنده ها

سرور های نامگذاری معمولا به حفظ اطلاعات کامل نام/ آدرس در مورد یک قلمرو خاص در فایلی به نام فایل ناحیه ای می پردازند. هر ناحیه می بایست سرور نام اولیه و ثانویه ای را برای بالا بردن انعطاف پذیری و توازن ظرفیت ها ایجاد کند. سرور مستر اصلی داده های مربوط به این نواحی را در فایل ناحیه حفظ می کند. تمام تغییرات در داده های ناحیه ای در پایگاه داده سرور اصلی روی می دهد. سرور ثانویه در فواصل معین به جستجوی سرور اصلی برای بروزرسانی رونوشت پایگاه داده می پردازد، و از اطلاعت برگشتی برای بروزرسانی پایگاه داده خود استفاده می کند. این فرایند به نام انتقال ناحیه ای می باشد پروتکل اولیه برای ارتباط DNS به نام UDP می باشد. به هر حال TCP (پروتکل کنترل انتقال)برای انتقال در ناحیه مورد استفاده قرار می گیرد و سرور های نامگذاری از UDP و پورت ۵۳ TCP برای جستجوی DNS پیروی می کنند.

در صورت غیاب اطلاعات دیگر، جستجوی تفکیک پذیر DNS همراه با جستجوهایی برای سرورهای نامگذاری اصلی آغاز شده، که به این معنی می باشد که سرور های نامگذاری بسیار شلوغ می باشند. ذخیره سازی به طور گسترده توسط تمام سرورهای نامگذاری برای کاهش ظرفیت در سرورهای اصلی مورد استفاده قرار می گیرد.

۲.۱ تفکیک پذیری جستجوی DNS

سرور نامگذاری به دو روش عمل می کند، بازگشتی و تکراری. جستجوی بازگشتی توسط علائم RD (برگشت مطلوب) ارسال شده که مرتبط به سرانداز جستجوی DNS می باشد. در روش بازگشتی سرور نامگذاری در بین زنجیره DNS در پاسخ به درخواست های دیگر به جستجو پرداخته و خطا یا پاسخ را برگشت می دهد، اما اشاره ای به سرورهای نامگذاری دیگر ندارد.

در مورد جستجوی تکراری، سرور نامگذاری جستجو کننده به روش تکراری عمل کرده و از پایگاه داده خود برای اطلاعات درخواستی استفاده می کند. اگر نتواند پاسخی را پیدا کند، معمولا آدرس IP نزدیک ترین سرور نامگذاری را می دهد که از نتایج آگاهی دارد. کلاینت درخواست را تکرار کرده، و در این زمان آن را به سروری می فرستد که در مورد آن آگاهی دارد. به طور پیش فرض، جستجوی سرور های نامگذاری ریشه تکراری می باشند.

۲.۲ فرمت پروتکل DNS

شکل ۱ فرمت جستجوی DNS و پیام های پاسخ داده شده را نشان می دهد. ما در زیر به بحث حوزه های مربوطه می پردازیم.

شکل ۱. فرمت پروتکل DNS

۲.۳ بایگانی منابع

بایگانی منابع (RRS) که در فایل های قلمرو سرور نامگذاری ذخیره می شوند، دارای فرمتی که در شکل ۲ نشان داده شده است می باشند.

Name	TTL	Class	Type	RDLength	RData

شکل۲. فرمت بایگانی منابع

نام دامنه به عنوان اشاره گر RR می باشد. زمان واقعی (TTL) مدت زمانی می باشد که RR ذخیره شده به شکل تایید شده می باشد. این رده به عنوان نوعی از شبکه می باشد؛ RRS معمولا مرتبط به رده IN (اینترنت) می باشد.

طول RDL مشخص کننده طول حوزه RDADA می باشد. در نهایت RDADA به شرح منابع با استفاده از فرمت مشخص شده توسط نوع و دسته می پردازد. RRSet به عنوان مجموعه ای از RRs صفر و یا بیشتر می باشد، که تمام آن ها دارای نان، دسته و نوع DNS یکسان می باشند.

۳- آسیب پذیری DNS

ما اکنون مختصرا به شرح چند نمونه از مهمترین حملات بر روی DNS می پردازیم. اکثر این مشکلات قبلا مورد بحث قرار گرفته اند.

۳.۱ حملات کاربری (MITM)

دریافت کننده اطلاعات از سرور نام DNS ، روشی در مورد تایید منشاء آن یا تایید یکپارچگی آن ندارد. این بدین دلیل

است که DNS به تعیین مکانیسم برای سرورها برای ایجاد جزییات موثق برای داده هایی که به سمت کلاینت می فرستند، نمی پردازد. تصمیم گیرنده هیچ راهی برای تایید و یکپارچگی اطلاعات ارسال شده توسط سرورهای نامگذاری ندارد.

تصمیم گیرنده تنها می تواند به تایید اصل بسته اطلاعاتی پاسخ داده شده DNS با استفاده از آدرس IP با استفاده از منبع DNS ،؛ مقصد و تعداد پورت منبع و شناسه تبادل DNS بپردازد. حمله کننده می تواند به راحتی بسته پاسخ سرور DNS را برای تطبیق این پارامترها ایجاد کند. کلاینت دارای هیچ انتخابی به غیر از اعتماد به داده های ایجاد شده توسط فرد مهاجم ندارد. مهاجم به تحلیل جستجوهای قانونی پرداخته، و با اطلاعات نادرست پاسخ می دهد.

۳.۱.۱ دریافت بسته

DNS درخواست یا واکنش کامل را به صورت مشخص و بسته UPD بدون رمز ارسال می کند، که ایجاد تغییرات در آن را آسان می کند. با دریافت بسته جستجوی DNS، پاسخ نادرست با سرعت برای ارسال به فرد تصمیم گیرنده قبل از اینکه پاسخ صحیحی از سرور نام ارسال گردد، ایجاد می شود. تطبیق روتر بر روی شبکه انتقال این امکان را برای فرد مهاجم ایجاد می کند تا بسته پاسخ داده شده DNS را از سرور نام دریافت کرده و آن را تغییر دهد. چون تایید منبع یا یکپارچگی داده پشتیبانی و یا بررسی نمی گردند، این موارد توسط تصمیم گیرنده آشکار نمی گردد.

۳.۱.۲ تخمین شناسایی مبادلات

مهاجم می تواند با پاسخ های نادرست نسبت به درخواست های پیش بینی شده بدون قرار گرفتن بر روی LAN(شبکه محلی) برای دریافت بسته ها، واکنش نشان دهد. این پاسخ ها توسط تصمیم گیرند یا سرور نام مورد نظر دریافت می گردد. حوزه شناسه مبادلات DNS یک میدان ۱۶ بیتی بوده و پورت UDP سرور که مرتبط با DNS می باشد، ۵۳ است. برای کلاینت تنها 2^{32} ترکیب احتمالی از شناسه (2^{16}) و پورت UDP کلاینت (2^{16}) برای کلاینت مورد نظر و سرور وجود دارد. عملا پورت UDP کلاینت و شناسه مبادله از جستجوهای قبلی پیش بینی می گردد. برای پورت کلاینت معمول می باشد تا مقدار ثابت شناخته شده ای بوده که این به دلیل محدودیت فایروال می باشد، یا تعداد پورت به طور فزاینده ای به دلیل عملکرد مجموعه افزایش می یابد. شناسه مبادله DNS توسط کلاینت معمولا به صورت پله ای افزایش می یابد. این باعث کاهش فضای جستجو در محدوده کمتر از (2^{16}) می گردد.

به این ترتیب، تخمین شناسه به اندازه ای نمی باشد که این امکان را برای مهاجم ایجاد کند تا داده های جعلی را رد کند. این فرایند با اطلاعات و تخمین ها در مورد جستجو (QNAME) و نوع جستجو (QTYPE) ادغام گشته که تصمیم گیرنده در حال جستجو می باشد. برای مثال این مورد، از طریق جستجوی حافظه نهان حاصل می گردد.

۳.۲ مشکلات ذخیره سازی

از طریق استفاده از حافظه نهان، DNS انطباق را قربانی کاهش زمانی دسترسی می کند. ذخیره سازی DNS نگرانی هایی را در مورد ناسازگاری ذخایر و بی ثباتی داده ها ایجاد می کند.

داده های قدیمی شامل اطلاعات حساس امنیتی می باشد. برای مثال موارد مهم در معرض خطر. پروتکل کنونی DNS از ابزارهای توزیع بروزرسانی داده یا باطل سازی سرور DNS یا موارد ذخیره سازی به روش سریع و ایمن پشتیبانی نمی کند.

۳.۲.۱ آلوده سازی حافظه نهان با استفاده از زنجیره نامگذاری

این حملات نشان دهنده اطلاعات نادرست در بخش ذخیره DNS می باشد. این موارد از طریق ابزارهای DNS RR حاصل می گردد که بخش RDATA آن شامل نام DNS بوده که به عنوان یک کد ماشینی برای قرار دادن داده های نامناسب مهاجمان در بخش حافظه نهان قربانی می باشد. مهمترین انواع موثر RR عبارتند از ,CNAME، NS،و DNAME RRs.

داده های نادرست مرتبط به این نام ها، به درون حافظه نهان قربانی از طریق بخش ها مازاد واکنش وارد می شود. مهاجم می تواند نام های DNS اختیاری را وارد کرده و اطلاعات بیشتری را فراهم کند که در ارتباط با ان نام ها می باشد.

۳.۲.۲ آلوده سازی حافظه نهان با استفاده از پیش بینی شناسه

در این حمله، تعداد زیادی از درخواست ها به سرور قربانی ارسال می شود (ns1.victim.com, say). که آدرس IP منبع را تغییر داده تا به تفکیک نام برای مثال به صورت

www.mybank.com بپردازد. هر یک از این درخواست ها در ارتباط با شناسه تبادل خاصی بوده و به طور مستقل پردازش می شوند. زمانی که ns1.victim.com در تلاش برای تجزیه هر یک از این درخواست ها می باشد، سرور در انتظار تعداد زیادی از درخواست ها از ns1.mybank.com می باشد.

مهاجم از این مرحله انتظار برای بمباران ns1.victim.com با پاسخ های جعلی از ns1.mybank.com استفاده کرده، و مشخص می شود که www.mybank.com اشاره ای به آدرس IP داشته که تحت کنترل فرد مهاجم می باشد. هر یک از این پاسخ های جعلی دارای شناسه مبادله مختلفی می باشد، یعنی پورت منبع و و آدرس IP سرور DNS جعلی (for ns1.mybank.com). حمله کننده انتظار دارد تا شناسه مبادله صحیح را حدس زده و پورت منبع توسط سرور نام جستجو مورد استفاده قرار می گیرد. اطلاعات جعلی در زمانی که حمله موفقیت آمیز بود، در حافظه نهان ns1.victim.com ذخیره می شوند.

۳.۳ حمله DDoS

DDOS دارای تاثیر قابل توجهی بر روی پایگاه DNS جهانی و کاربران ان دارد. آن ها معمولا در سرورهای اصلی قرار می گیرند. این موارد با حملات DDOS اخیر در ژوئن ۲۰۰۴ نشان داده می شود، که تکرار حملات مشابه اکتبر ۲۰۰۲ می باشد. این حملات منجر به عدم دسترسی پذیری سرویس تفکیک نام نسبت به جوامع اینترنتی می گردد.

۳.۴ حملات DNS مهم دیگر.

۳.۴.۱ نفوذ اطلاعات

انتقال موفق توسط فرد مهاجم بر مبنای حمله شناسایی می باشد، که به صورت بلقوه اطلاعات حساس را در مورد پیکره بندی شبکه داخلی ، برای مثال، آدرس های IP رابط فایروال اینترنتی نشان می دهد. برای مثال نام DNS، نشان دهنده نام پروژه می باشد که برای فرد مهاجم دارای مزایایی بوده، یا نشان دهنده هویت سیستم عامل اجرایی بر روی دستگاه می باشد.

۳.۴.۲ آسیب پذیری بروزرسانی پویای DNS

پروتکل هایی همانند پروتکل پیکره بندی میزبان پویا (DHCP) از پروتکل بروزرسانی پویای DNS برای اضافه و حذف RRS بنا به درخواست استفاده می کند. این بروزرسانی در سرور اصلی قلمرو روی می دهد. تایید چنین بروزرسانی منحصرا بر مبنای آدرس IP منبع می باشد، و برای تهدیداتی همانند جعل IP آسیب پذیر می باشند. این حملات در محدوده رد سرویس، شامل حذف سوابق برای تعیین جهت می باشد.

۳.۵مد نظر قرار دادن امنیت پیوند

سرور های DNS در اینترنت که از پیوند اجرایی نرم افزار DNS استفاده می کنند همیشه با وصله های امنیتی و بروزرسانی نرم افزار همگام نمی باشند. در نتیجه، در هر زمان، بخش قابل توجهی از سرور DNS اینترنت آسیب پذیر می باشد. اکثر این آسیب پذیری ها در نتیجه اجرای ضعیف و بررسی محدود می باشد. بهره برداری از آن به طور بلقوه ای این امکان را به فرد مهاجم می دهد تا کدهای اختیاری را به اجرا در آورده یا داده ها را در محل های اختیاری در حافظه بنویسد.

۳.۶ آسیب پذیری کاربرد

استفاده از DNS شرایطی برابر با حملات DDOS را تحریک می کند. نسبت جستجوی DNS در سرور اصلی از یک جستجو در هر ثانیه به تقریبا ۱۰۰۰۰ جستجو در ثانیه در سال ۲۰۰۴ می رسد. اندازه گیری در سرورهای اصلی تعداد قابل توجهی ازجستجوهای جعلی را نشان می دهد: ۶۰ تا ۸۵٪ از جستجوهای مورد نظر از میزبان مشابهی در فاصله اندازه گیری تکرار می گردد. بیش از ۱۴٪ از ظرفیت جستجوی سرور اصلی بر مبنای جستجوهایی می باشد که باعث نقص خصوصیات DNS می گردد.

سرور اصلی تعداد زیادی از درخواست را دریافت می کند، زیرا تصمیم گیرنده پاسخ ها را دریافت کرده، و این به دلیل فیلترهای بسته و موضوعات مسیریابی می باشد. کاربرد و رمزگذاری نامناسب کلاینت تصمیم گیرنده منجر به تاثیر DDoS بر روی سرورهای اصلی DNS می گردد.

۴- توسعه امنیت سیستم نام دامنه (DNSSEC)

DNSSEC امنیت را به پروتکل DNS با ایجاد تایید اصل، یکپارچگی داده و عدم پذیرش مشخص وجود داده های DNS ایجاد شده توسط سرور نام اضافه می کند. تمام پاسخ های حاصل از سرور DNSSEC به صورت دیجیتالی تعیین می گردند. با بررسی این علائم، تصمیم گیرنده DNSSEC قادر به بررسی این موضوع می باشد که آیا اطلاعات حاصل از سرور قانونی می باشد و اینکه داده ها مشابه داده ها در سرور DNS

تایید شده می باشد. اگر داده ها بر روی سرور نشان داده نشود، عدم پذیرش بوجود می آید.

برای حفظ سازگاری برگشتی با DNS، DNSSEC تنها نیازمند تغییرات جزئی بر روی پروتکل DNS می باشد. که به نام های علائم ثبت منابع (RRSIG)، کلید عمومی DNS (DNSKEY)، امضای تایید کننده (DS)، و امنیت بعدی (NSEC) می باشند. DNSSEC از دو بیت نشانه استفاده نشده قبلی در جستجوی DNS و سرپایم پاسخ ها استفاده می کند. (AD و CD). بیت AD (داده های معتبر) در پاسخ نشان دهنده این می باشد که تمام داده های قرار گرفته در پاسخ و بخش تایید شده پاسخ ها توسط سرور تایید می شوند. بیت CD (بررسی های نامشخص) نشان می دهد مکه اطلاعات نامعتبربرای تصمیم گیرنده ای که این درخواست ها را ارسال می کند قابل قبول است. چون پروتکل UDP دارای محدودیت اندازه بسته۵۱۲ بیت می باشد، DNSSEC نیازمند استفاده از تعمیم EDNS0 می باشد که بر روی این محدودیت ها غلبه می کند. بنابراین اندازه های کلیدی بزرگتر مورد قبول می باشد.

DNSSEC قابلیت آشکار کردن حملات MITM را بر روی DNS از طریق افزودن تایید داده اصلی، انتقال و تایید درخواست نشان می دهد، اما DNSSEC از چنین حملاتی جلوگیری نمی کند. برای حفظ صحت اصل داده و یکپارچگی آن ها، هر دو مورد یعنی سرورها و تصمیم گیرندگان می بایست از پروتکل DNSSEC استفاده کنند.

۴.۱ موارد کلیدی در DNSSEC

هر منطقه امنیتی دارای زوج کلیدی می باشد که متشکل از کلید خصوصی منطقه و کلید عمومی منطقه می باشد. کلید عمومی منطقه به عنوان ثبت منابع ذخیره می گردد. کلید عمومی توسط سرورهای DNS و تصمیم گیرنده برای تایید علائم دیجیتال منطقه مورد استفاده قرار می گیرند.

تمام منابع ثبت شده در منطقه امنیتی توسط ملید خصوصی منطقه نشان داده می شوند. برای اینکه نشان گذاری منطقه و گردش کلیدها را آسان تر کنیم، این امکان وجود دارد تا از یک یا چند کلید بر مبنای کلیدهای علامتگذاری (KSKs) استفاده کنیم.

KSK تنها برای تعیین KEY RRs سطح بالا در یک منطقه مورد استفاده قرار می گیرد. کلیدهای علامت گذاری شده منطقه ای (ZSKs) برای تعیین مجموعه های RR در یک منطقه مورد استفاده قرار می گیرند.

۴.۲ علائم در DNSSEC

DNSSEC موارد تایید شده متغیری را از مجموعه RR با مرتبط ساختن آن با ثبت منابع مشخص ایجاد می کند که باعث پیوند اطلاعات DNS با فاصله زمانی و نام دامنه تایید کننده می شود.

کلید خصوصی برای تعیین مجموعه RR مورد استفاده قرار می گیرد. در ارتباط با سرعت افزایشی ترکیبی از مجموعهRR مد نظر قرار می گیرد. این باعث ایجاد منشاء اطلاعات تایید شده می باشد. اگر اطلاعات در زمان انتقال تغییر یابد، علائم دیگر معتبر نمی باشند (یکپارچگی اطلاعات تایید شده). در مورد DNSSEC، تنها علائم مورد استفاده قرار گرفته و هیچ چیز به طور رمز شده نمی باشد.

این ترکیبات با استفاده از MD5 یا SHA-1 ایجاد می گردند. علائم با استفاده از MD5/RSA، DSA یا الگوریتم نهفته منحنی بیضی شکل ایجاد می شود. این علائم بر مبنای ثبت منابع (نوع RRSIG) ذخیره شده و در کلید خصوصی محدوده برای تایید ثبت منابع مورد استفاده قرار می گیرند.

۴.۳ ثبت NSEC

هر نام مشخص بر مبنای منطقه امن می باشد که بر مبنای ثبت منابع NSEC مشابه مد نظر قرار می گیرد، که اشاره ای به نام های بعدی نشان داده شده در منطقه دارد. زنجیره متوالی ثبت منابع NSEC برای یک منطقه نشان می دهد که چه منابع ثبت شده ای در واقع وجود دارد. ثبت منابع NSEC توسط کلید خصوصی آن منطقه تعیین شده، و از در معرض خطر افتادن منطقه از طریق شرایط تایید نشده یا حذف شدن ثبت منابع در منطقه جلوگیری می کند. ثبت منابع NSEC برای یک ناحیه به صورت اتوماتیک زمان ایجاد می گردد که ثبت ناحیه مد نظر قرار گیرد.

۴.۳.۱ زمان در DNSSEC

تمام زمان ها در DNS نسبی می باشند. تایید منابع ثبت شده (SOA) تقویت شده، بررسی مجدد و زمان انقضا بر مبنای شمارشگرهایی می باشند که برای تعیین زمان سپری شده شناسایی شده، از این رو سرور پیرو هماهنگ با سرور اصلی می گردد. مقدار زمان تعیین شده (TTL) برای تعیین این مورد به

کار می رود که چگونه یک فرستنده می بایست اطلاعات را بعد از اینکه از یک سرور مشخص ارسال شدند، ذخیره کند. DNSSEC زمان مطلق را در DNS معرفی می کند.

دوره اعتبار علائم دوره ای می باشد که یک علامت تایید می شود. آن در زمانی شروع می شود که در بخش ابتدایی علائم RRSIG شروع شده و در زمان مشخصی به انقضا می رسد. دوره انتشار این تایید ها زمانی می باشد که یک علامت جایگزین موارد منتشر شده RRSIG در فایل اصلی می گردد.

۵- آسیب پذیری DNSSEC

DNSSEC در برابر پیکره بندی ضعیف و اطلاعات نادرست در سرور نامگذاری تایید شده حمایت نمی شود، و در برابر حملات بافر یا DDOS حمایت نمی شود. افزایش قابل توجه در ظرفیت محاسباتی بر روی سرور و تصمیم گیرنده، مدل زنجیره ای اعتماد، فقدان ابزار مدیریتی، و نیاز برای سطح بالای هماهنگی بین سرور ها به عنوان یکی از مهمترین موانع برای کاربرد می باشد.

موضوع مدیریت کلیدهای نهفته، همانند پیکره بندی کلید اولیه و معکوس کردن بخش های کلیدی در سطح عملیاتی مد نظر قرار گرفته تا DNSSEC را برای بکارگیری در مقیاس جهانی توانمند سازد. ذخیره کلید خصوصی منطقه به عنوان مسئله دیگر بوده، و DNSSEC نمی تواند نقایص سرور را تحمل کند. در نهایت همان زور که تجارب ازمایشگاهی SECREG نشان می دهد، DNSSEC براتی اجرا پیچیده می باشد.

۵.۱ زنجیره اعتماد

DNSSEC دارای مدل اعتماد زنجیره ای می باشد. برای تفکیک امنیتی نام در ,DNSSEC، کلید عمومی اصلی می بایست در تصمیم گیرنده موجود باشد. کلید عمومی با پیکره بندی آماری در سرور DNS یا تصمیم گیرنده یا از طریق کلید های خصوصی ناحیه ای تعیین می گردند.

زنجیره فعالیت های مدیریت شده با در نظر گرفتن بخش های امنیتی به نام علائم وکالتی (DSs) می باشند. ثبت DS اعتماد را از بخش های مادر به بخش های کلیدی ثانویه می برد. موارد ثبت شده DS باعث نگه داشتن کلیدهای عمومی SHA-1 می گردد. با بررسی علائم ثبت شده DS ، تصمیم گیرنده می تواند به تایید موارد ادغام شده کلید عمومی بپردازد و به این ترتیب می تواند به تایید کلیدهای عمومی بپردازد.

حملات تزریق شده کلید عمومی از نقطه نظر کلاینت ، منطبق با این زنجیره اعتماد می باشد. انطباق در هر ناحیه بین ریشه و نام هدف خاص منجر به اطلاعاتی می گردد که به صورت جعلی بوده که باعث می شود کل دامنه های فرعی برای کلاینت های مورد نظر ناهویدا گردند.

داده هایی که در سرور اولیه تایید شده منتشر می گردند، فورا توسط کلاینت ها تعریف نمی گردند. مدت زمانی طول می کشد تا اطلاعات به سرورهای نام معتبر دیگر منتقل گردند. در طی این دوره، کلاینت ها اطلاعات را از سرورهای معتبر دریافت می کنند.

در ارتباط با کلاینت های معرفی شده، این مساله حائز اهمیت می باشد که داده های حاصل از مناطق امنیتی برای ایجاد زنجیره اعتماد مورد استفاده قرار گیرد بدون توجه به اینکه این اطلاعات به طور مستقیم حاصل از سرورهای موثق یا سرور نام ذخیره شده باشد.

۵.۲ موضوعات امنیتی برای کلیدها

اندازه کلید، الگوریتم و دوره تایید می بایست با دقت انتخاب شود. دوره تایید کلیدی چندین موضوع را با توجه به ساخت، مدت زمان، اندازه و ذخیره کلیدهای خصوصی تحت تاثیر قرار می دهد. زمانی که اندازه های کلیدی انتخاب می شود، بخش های اجرایی می بایست دوره اعتبار کلیدی را مد نظر قرار داده و اینکه چه اطلاعاتی در طی این دوره مشخص می گردد.

۵.۲.۱ معکوس کردن کلید

هر چه کلید های طولانی تری مورد استفاده قرار گیرد، احتمالات بیشتری ایجاد می گردد که این موارد از طریق بی توجهی، تصادف، جاسوسی یا کشف رمز منطبق گردند.

در زمان معکوس کردن کلید، اطلاعات منتشر شده در مورد نسخه مناطق در بخش های پنهان همچنان وجود دارند. نادیده گرفتن اطلاعات ذخیره شده قبلی منجر به از دست رفتن سرویس برای کلاینت می گردد، به ویژه زمانی که مواد نواحی توسط کلیدهای قدیمی تعیین شده و توسط تصمیم گیرنده ها تایید می گردند که دارای مناطق قدیمی کلیدهای ذخیره شده نمی باشند. اگر کلیدهای قدیمی دیگر در مناطق جاری موجود نباشند، این ارزیابی رد می گردد، که نشان دهنده جعل اطلاعات می باشد. همچنین تلاشی انجام می گیرد تا به تایید داده ها بپردازد که توسط کلیدهای جدید در برابر کلیدهای قدیمی مشخص گشته که در بخش های ذخیره محلی قرار داشته و

منجر به داده هایی می شوند که به صورت ساختگی مد نظر قرار می گیرند.

دسترسی به معکوس کردن کلید در ریشه پیچیده می باشد که به این ترتیب کل پایگاه داده پیوسته را تحت تاثیر قرار می دهد. فعالیت هایی می بایست انجام گیرد تا به طور مشخص به تعیین این موضوع بپردازد که چگونه کلید اصلی معکوس می گردد.

۵.۲.۲ ذخیره کلید خصوصی قلمرو

DNSSEC نشان می دهد که کلید خصوصی منطقه می بایست به شکل آفلاین مد نظر قرار گیرد. این موارد موضوعاتی را مطرح می کند که پشتیبانی را از بروز رسانی پویا انجام داده، به گونه ای که کلید خصوصی ناحیه برای ایجاد علائم (RRSIG) به صورت تمام وقت برای تایید پویای داده های بروزشده مورد استفاده قرار می گیرد. این فرایند داده های بروز شده پویا را در DNSSEC به صورت غیرقابل دسترس و اتلاف شده در می اورد قبل از اینکه نشانه گذاری منطقه بعدی از کلیدهای خصوصی نواحی استفاده می کند.

نقص امنیتی سرور که کلیدهای خصوصی نواحی را ذخیره می کند به فرد مهاجم اجازه دسترسی کامل به قلمرو می دهد. برای اطمینان از امنیت کامل، کلیدهای خصوصی منطقه، هرگز در حافظه سرور قرار نمی گیرند.

۵.۲.۳ موضوعات زمان بندی DNSSEC

DNSSEC شرایطی را برای هماهنگی زمان بین تصمیم گیرنده و میزبان که به ایجاد علائم DNSSEC می پردازند ایجاد می کند. تصمیم گیرنده می بایست مفهوم مشابهی از زمان مطلق داشته باشد تا تایید کند لین علائم تایید شده می باشند یا منقضی شده اند. مهاجمی که بتواند عقیده تصمیم گیرنده را از زمان مطلق جاری تغییر دهد، می تواند تصمیم گیرنده را در استفاده از علائم منقضی شده گول بزند. مهاجم که بتواند ذهن قربانی را در مورد زمان مطلق تغییر دهد، می تواند این افراد را در ایجاد علائمی که دوره تایید ان ها منطبق با آنچه که فرد در ذهن دارد، فریب دهد.

علائم (RRSIG) تنها بر مبنای جستجو ایجاد نمی گردند، اما در عوض بعضی اوقات توسط ttl سطح بالا ایجاد می گردند، به صورتی که علامت گذاری یک فرایند بر مبنای گسترش منابع می باشد. این فرایند دید وسیعی را در ارتباط با حملات جدید ایجاد می کند، به صورتی که داده های قدیمی که علائم مرتبط به ان ها هنوز منقضی نشده اند تکرار می گردند تا کلاینت را گمراه کنند.

SIG RRs از زمان آغاز مجموعه علائم از پیش تعیین شده تا زمان انقضا مد نظر قرار می گیرند. به نظر می رسد که این فاصله زمانی زیاد باشد. rrl مشابه معتبر می باشد تا زمانی که زمان انقضا علائم یا زمان انقضای TTL، به هر روشی که باشد، در ابتدا می آید. حتی اگر RR بروز باشد، بروزرسانی واقعی تا زمان انقضای TTL یا علائم به صورت نامشخص می باشد. DNSSEC نیازمند هماهنگی زمانی بین سرور های نام اولیه و ثانویه می باشد.

۵.۲.۴ مکانیسم اثبات کاراکتر

کاراکتر (*) که در حوزه نام RR مورد استفاده قرار می گیرد، این امکان را برای موارد ثبت شده ایجاد می کند تا برای موارد ثبت شده دیگر مشخص گردند (از نوع یکسان، اشاره به داده های یکسان، در منطقه مشابه). نام کاراکتر به عنوان الگویی برای ترکیب RR به طور پیوسته می باشد که بر طبق به قوانین منطبق می باشد. کاراکتر MX RRs در سطح گسترده ای مورد استفاده قرار می گیرد.

وجود نماد RR، و عدم وجود RRs در صورت وجود، کاراکتر RR را بی نظم می کند (بر طبق به قوانین ترکیبی) که می بایست اثبات گردند. این باعث می شود که مکانیسم اثبات کاراکتر وابسته به مکانیسم رد تایید باشد. DNSSEC به اثبات کاراکترها که در بالا توصیف شده است می پردازد.

۵.۲.۵ ظرفیت محاسباتی سطح بالا

DNSSEC به طور قابل توجهی باعث افزایش اندازه بسته واکنش DNS می گردد، که به طور قابل توجهی ظرفیت محاسبه را بر روی سرور های DNS بالا برده و زمان واکنش جستجو را بالا می برد.

فرایند تایید ثبت منابع از نظر محاسباتی به ویژه برای اندازه های کلیدی بزرگتر، بالا می باشد. استاندارد DNSSEC به اندازه ۱۰۲۴ بیت کلید را امکان پذیر می سازد. افزودن علائم دیجیتالی به یک دامنه اندازه موارد ثبتی را ۵-۷ برابر افزایش داده، که هزینه را بر روی سرورهای نام بالادست قرار می دهد.

تایید پاسخ DNSSEC حجم کار تصمیم گیرنده را بالا برده، از این رو تصمیم گیرنده DNSSEC نیاز به اجرا تایید علائم دارد و، در بعضی از موارد، نیاز به جستجوهای بیشتری دارد. این

افزایش حجم کار باعث افزایش زمان می گردد که پاسخ را به سمت کلاینت DNS اصلی می برد.

۵.۲.۶ فقدان ابزارهای مدیریتی

DNSSEC به طور قابل توجهی پیچیده تر از DNS می باشد. تنها ابزارهای کمی برای کمک به فعالیت حفظ دامنه علائم وجود دارد. ارزیابی DNSSEC و ابزارهای تحلیلی ثبت وقایع همچنان توسعه یافته می باشند. اشکال زدایی به صورت دستی به عنوان یک فعالیت زمان برو پیچیده می باشد.

۵.۲.۷ فقدان کنترل هماهنگی

DNSSEC از یک طرح اولیه و ثانویه ساده برای ایجاد قابلیت دسترسی سرور و توزیع ظرفیت استفاده می کند. تنها یکی از سرور نام ثانویه و اولیه در جستجوی خاص نقش دارند. یک سرور در معرض خطر برای مسدود کردن، دزدیدن، یا اطلاعات غیرمستقیم و درخواست بروزرسانی موضوعات پیچیده کافی می باشد. بروزرسانی داده تنها در سرور اصلی روی می دهد، و سرور ثانویه از بروزرسانی تا زمان انتقال قلمرو بعدی آگاه نمی گردد . بنابراین ناسازگاری بین وضعیت سرور اصلی و ثانویه وجود داشته، و جستجوی کلاینت منجر به جواب های کاملا متفاوتی می گردد که بستگی به این موضوع دارد که کدام سرور جستجو را انجام می دهد. این فرایند منجر به ناسازگاری و مشکلات قابلیت اطمینان حتی بدون حمله بین المللی می گردد.

۵.۲.۸ آسیب پذیری منطقه DNSSEC NSEC

NSEC برای اثبات تایید شده عدم وجود DNS RRs مورد استفاده قرار می گیرد. به معرفی قابلیت گروه های مخالف برای شمارش تمام نام ها در منطقه با دنبال کردن زنجیره NSEC می گردد. NSEC RRs نشان می دهد که چه نام هایی در قلمرو با پیوند نام های کنونی نسبت به نام های موجود در مسیر ترتیب استاندارد درون یک منطقه قرار ندارند. فرد حمله کننده می تواند به جستجوی NSEC RR ها به طور متوالی برای دریافت تمام نام ها در منطقه بپردازد. این فرایند به حمله کننده این امکان را می دهد تا شمارش قلمرو بپردازد.تکنیک های همچون پوشش حداقل ثبت NSEC و NSEC3 برای حل این مشکلات مطرح می شوند.

۵.۲.۹ مشکلات DNSSEC در NL.

SEGREG بر مبنای بررسی DNSSEC بوده که توسط NLNetLabs به اجرا در می آید. در طی آزمایش یکی از موارد ثانویه nl (dnssec.nic-se.se) به دلیل سرریز شدن حافظه برای بیش از دو هفته بروز نمی گردد. این باعث ایجاد مشکلات جدی می گردد. علائم طول مدت برای nl. برابر با یک هفته بوده، و به این ترتیب علائم مربوط به nic-se.se تماما منقضی می گردند. کاربران این سرور داده های نامناسبی را برای .nl. با DNSSEC, مد نظر قرار داده، موارد ثانویه ای برای مدت زمانی مشخصی بروز نمی باشند باعث حذف محلی دامنه ها می گردند.

۶- خلاصه و نتیجه گیری

DNS دارای موضوعات امنیتی مهمی بوده که ضرورتا مد نظر قرار می گیرد. تهدیداتی همانند کاربر در خلال حمله و حمله حافظه نهان در DNS به دلیل نبود تایید و یکپارچگی در فرایند انتقال DNS ایجاد می گردد. بررسی محدوده نادرست و غیر وجودی و شرایط مدیریت خطا در نرم افزار BIND منجر به موارد به کارگرفته شده همانند به جریان انداختن بافر می گردد. تهدیدات کاربردی توسط مجموعه ای از مدخل ها از کلاینت غیرپیکره بندی شده تا فیلتر بسته ها ایجاد شده که منتهی به شرایط همانند DDoS می گردد.

کارگروه مهندسی اینترنت (IETF) به این تهدیدها با توسعه DNSSEC ، یک پروتکل DNS ایمن پاسخ می دهد. DNSSEC امکان سطح مبادله و انتقال منطقه ایمن که از تمام داده ها در قلمرو در طی انتقال حمایت می کند، ایجاد می کند. در DNSSEC, حملات بر مبنای نام آشکار می گردد.

DNSSEC در برابر انبوه بافرها یا حملات DDoS حمایت نشده، و همچنین موارد خیلی محرمانه را مشخص نمی کند. اعطای امنیت برای اجرا بسیار پیچیده بوده و قابلیت گزارش خطای DNSSEC's حداقل می باشد. فایل منطقه ای DNSSEC به طور قابل توجهی بزرگتر از همتای DNS می باشد. که شامل بارگذاری بر روی سرور، شبکه و تصمیم گیرنده می باشد.

کلیدهای عمومی و خصوصی که توسط DNSSEC مورد استفاده قرار می گیرند با گذشت زمان در معرض خطر قرار می گیرند. کلیدها در این فواصل برای کاهش ریسک خطر تغییر می یابند. این موارد نسبتا در سطوح پایین تر زنجیره DNSSEC به اسانی به اجرا در می آیند، به گونه ای که برای مدت زمان طولانی ذخیره نمی گردند. معکوس کردن کلید اصلی دارای تاثیر قابل توجهی بر روی ساختار کلی DNSSEC می باشد. انتخاب

پارامترهای زمان بندی در ,DNSSEC مهم بوده، که شامل TTL، زمان آغاز علائم و زمان انقضای علائم می باشند.
با وجود این آسیب پذیری ها در DNSSEC، یکپارچگی و تایید در ارتباط با داده های DNA ایجاد می گردد.
DNSSEC دارای تناسبی با زیرساخت های DNS کنونی می باشد. ما تحقیقات بیشتری را در حوزه هایی همانند پروتکل انتقال قلمرو پویا پیشرفته با استفاده از الگوریتم های نوع پیوندی ، یکپارچگی ریشه های ذخیره، با ریشه ICANN برای ایجاد فرا ریشه ، حالت ارتجاعی DNSSEC، حملات فعال در برابر سرویس های راهنمای توزیع شده همانند X.500 ، پروتکل دسترسی دایرکتوری سبک (LDAP)، و کربروس، DNSSEC بر روی ابزارهای موبایل و ,MANETs، و حفاظت از DDoS در برابر ,DNSSEC برای بهبود عملکرد اصلی DNSSEC، نشان می دهیم.

مراجع

[1] مقالهDNSSEC - Nicolas T.capalbo - Cs6 Professor Schaumann 2011/5/4
[2] مقالهDNSSEC Tutorial - Will.i.am Hervey Allen -February 21, 2011
[3] Configuring Windows server MCTS self-paced training c2008.2008 active directory , Ruest, Nelson