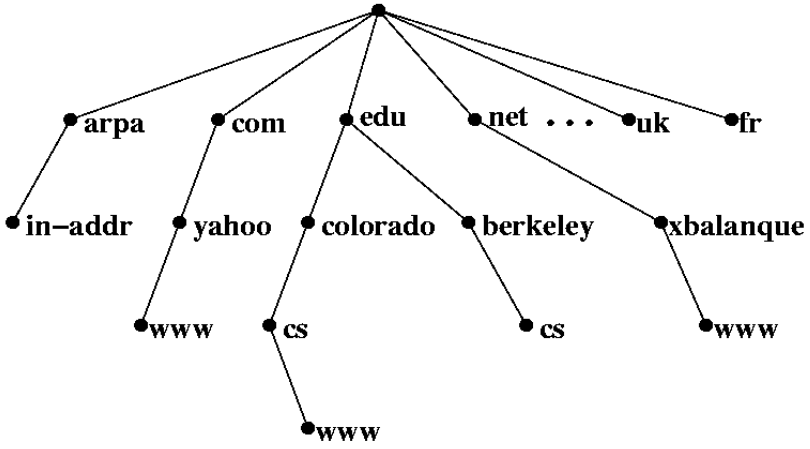
حماية نظام أسماء النطاقات
DNS Security (DNSSEC)

أولا : مقدمة

من المعروف أن جميع الأجهزة علي شبكة الأنترنت لها عنوان وحيد وهذا العنوان يطلق علية IP Address وهو مكون من أربع مقاطع وتتراوح قيمة كل مقطع من 0 حتي 255 مثال 192.168.0.100 ، ويمكن الوصول إلي أي جهاز عن طريق هذا الرقم ، ومن الصعوبه بمكان إستخدام IP في التعاملات لذلك فانه يتم إعطاء إسم وحيد لكل عنوان حيث يتم التعامل مع هذا الإسم عوضاً عن IP مثل موقع www.google.com فإن عنوانه علي شبكة الإنترنت 216.239.59.99 ولكن كيف تتم عملية تحويل الأسماء إلي العناوين المقابله لها لان الأصل في التعامل هو العنوان وليس الإسم ومن هنا بدأت فكرة تكوين ما يسمي "نظام أسماء النطاقات" DNS (Domain Name System) حيث يتم من خلال هذا النظام تحويل الأسماء إلي العناوين وتسمي هذه العملية Address Resolution وبالعكس يمكن الحصول علي إسم النطاق بمعلومية العنوان ، ويمكن توضيح هذا الأمر بشكل بسيط كالاتي

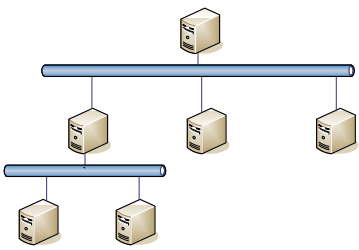
1- يتم كتابة إسم الموقع www.google.com في المتصفح .
2- يتم البحث في الجدول الخاص بأسماء النطاقات عن www.google.com .
3- في حالة العثور علي الإسم يتم ارجاع العنوان الخاص بالموقع .

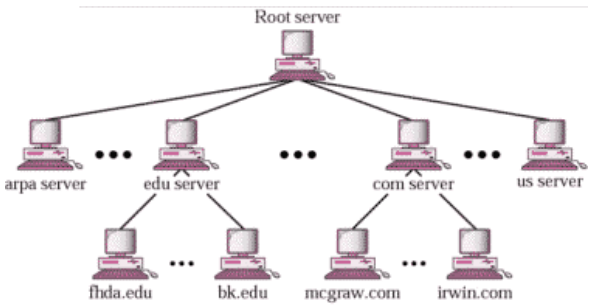
الإسم	العنوان
www.example.com	211.215.20.1
www.google.com	216.239.59.99
.....	.....



تخزن أسماء النطاقات داخل النظام بشكل شجري

ومن الممكن أيضا إجراء العملية السابقة بشكل عكسي أي أنه يمكن معرفة إسم النطاق بإستخدام العنوان ويمكن الإستفادة من هذا النظام لتقديم خدمة الإستعلام عن النطاقات والمعلومات الخاصة بها والتاكد من عدم إستخدام هذا النطاق من قبل جهة أخري.
ونظرا لضخامة بيانات أسماء النطاقات فإنه يتم تحزين هذه البيانات بعدة ملقمات Servers ملقم رئيسي وفرعي وهكذا .





ملقمات DNS

وبهذا الشكل يمكننا الحصول علي عنوان موقع www.google.com كالاتي

1- يتم كتابة إسم الموقع www.google.com في المتصفح .
2- يتم البحث داخل الملقم الرئيسي عن أسم النطاق www.google.com .
3- في حالة العثور علي الإسم يتم أحد الأمرين
   a. الحصول مباشرتا علي العنوان الخاص بالإسم
   b. الإحالة إلي ملقم أخر يحتوي علي الإسم
4- وهكذا تتكرر العملية أ ، ب في الخطوة السابقة حتي يتم الوصول إلي عنوان الموقع.

ومن الواضح أن أي خلل في هذا النظام قد يسبب إرباك للمستخدمين فمثلا إذا تم إختراق هذا النظام بشكل أو بأخر وتم تغير عنوان موقع ما فإن المستخدم الذي سيقوم بإستخدام الإسم لتصفح الموقع سوف يتصفح موقع أخر ومن هنا تأتي أهمية حماية هذا النظام والذي يعرف بحماية نظام أسماء النطاقات DNS Security .

ثانيا : آلية عمل "نظام أسماء النطاقات" DNS

كان المسؤل عن متابعة وتحديث معلومات أسماء النطاقات حول العالم هو معهد
Stanford Research Institute's Network Information Center (**SRI-NIC**)
وكانت الطريقة المتبعة من قبل SRI-INC هي إنشاء ملف ضخم يسمي hosts.txt حيث يحتوي علي جميع أسماء النطاقات والعناوين ويقوم SRI-NIC بتحديثه ورعايته بشكل دوري .
ومع إتساع شبكة الأنترنت ونمو عدد المواقع فقد أصبح من الصعب متابعة وصيانة نظام أسماء النطاقات DNS بهذه الطريقة ولذلك فقد تم إعتماد آلية أخري وهي توزيع أسماء النطاقات علي ملقمات في صورة قواعد بيانات يمكن صيانتها وتحديثها بشكل أسهل وأسرع وقد ساعد هذا البناء علي تحسين أداء نظام أسماء النطاقات DNS بشكل كبير وهذا هو المتبع الان وبهذه الطريقة أصبح نظام DNS غير مركزي بمعني أن معلومات أسماء النطاقات موزعة علي مجموعة من الملقمات .

ثالثا : تطبيقات "نظام أسماء النطاقات" DNS Implementation

من أشهر التطبيقات علي شبكة الأنترنت لنظام أسماء النطاقات DNS هو Berkeley Internet Name Daemon (**BIND**)
وهذا التطبيق يحتوي علي برامج خاصة بالملقمات Servers والأجهزة الطرفية Clients وكذلك مجموعة من الأدوات المساعدة للصيانة والدعم ، وقد أصبح هذا التطبيق في يومنا هذا الأشهر في العالم .

رابعا : تهديدات "نظام أسماء النطاقات" Threats to the Domain Name System

إن نظام أسماء النطاقات DNS تم بناءه في الأصل لهدف تحويل أسماء النطاقات إلي العناوين والعكس ولكن هذا النظام لم يعني في البداية ببناء نظام أمني للتأكد من صحة الإجابات التي يصدرها النظام ولذلك فقد ظهر في بعض الأوقات خلل بهذا النظام مما أدي إلي إحداث فوضي علي الأنترنت .
ويمكن عرض الثغرات أو الخروقات التي يتعرض لها نظام أسماء النطاقات DNS إلي عدة مستويات

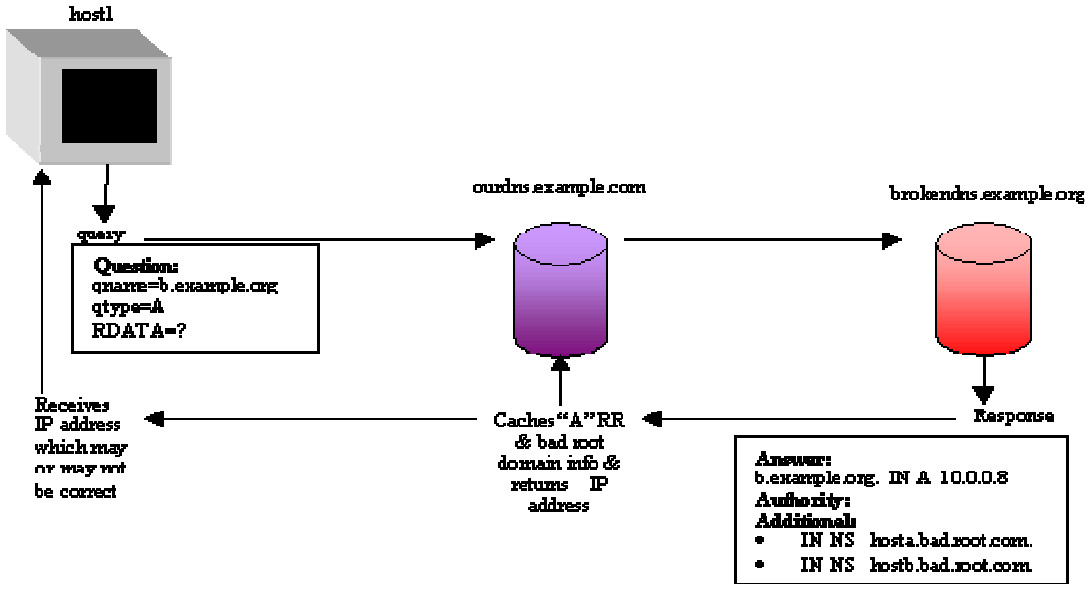
أ- تلوث الذاكرة المؤقتة Cache Poisoning

كما ذكرنا سبقا فإن طريقة عمل نظام أسماء النطاقات DNS يعتمد علي وجود ملقم رئيسي وملقمات وفرعية وسوف نستعرض الأن دور ما يسمي بالذاكرة المؤقتة في النظام ، فمثلا إذا تم الإستفسار عن عنوان موقع www.example.com فأنه

1- يتم الإستعلام عن عنوان الموقع في الملقم الرئيسي Root Server وفي حالة الإحالة إلي ملقم فرعي فأنه يتم إنتظار رد الملقم حيث يقوم الملقم الفرعي بالبحث داخل قاعدة البيانات وفي حالة الحصول علي العنوان يتم إرسال النتيجة إلي الملقم الرئيسي وفي حالة الإحالة إلي ملقم فرعي أخر يتم إنتظار الرد وهكذا حتي يتم الحصول علي العنوان ويتم ارسال العنوان إلي الملقم الرئيسي .

2- ماذا لو تم الإستفسار مرة أخري عن عنوان الموقع www.example.com هل سيقوم الملقم الرئيسي بنفس الخطوات السابقة مرة أخري ، هنا يظهر دور ما يسمي "بالذاكرة المؤقتة " Cache ويتلخص دور الذاكرة المؤقتة في الأحتفاظ بنتائج البحث السابقة وفي حالة الإستفسار مرة أخري عن نفس العنوان فإنه يتم التأكد أولا من قاعدة البيانات الموجودة بالملقم وفي حالة عدم الحصول علي العنوان فإنه يتم التأكد من الذاكرة المؤقتة وفي حالة العثور علي الإجابة يتم الرد بناء علي البيات الموجودة بالذاكرة المؤقتة .

ويتضح من المثال السابق أن دور الذاكرة المؤقتة هو تحسين أداء النظام ، وتمكن الخطورة في هذه العملية في حالة إختراق نظام الذاكرة المؤقتة وتم تغير البيانات بداخلها ففي هذه الحالة سيقوم الملقم الرئيسي بإستخدام هذه البيانات الخاطئة وبالتالي سنحصل علي نتيجة غير صحيحية للإستفسار بمعني أخر أنه في حالة الإستعلام عن عنوان الموقع www.example.com قد نحصل علي عنوان موقع أخر أو عنوان غير موجود .وتسمي هذه العملية "بتلوث الذاكرة المؤقتة" **Cache Poisoning**



ب- إغمار الجهاز العميل Client Flooding

تحدث عملية إغمار جهاز العميل Client Flooding في حالة القيام بتوجية إستفسار إلي الملقم ويتم إستقبال آلاف الردود من النظام DNS ولكن هذه الردود مرسلة من قبل مهاجمين والمشكلة أنه لا توجد آلية للتأكد من مصداقية هذه الردود أي لا يمكن التاكد ما إذا كانت هذه الردود واردة بالفعل من الملقم أو من أحد المهاجمين وفي هذا السبب يكمن نجاح المهاجم في إختراق النظام .

ت- الحلّ الوسط لبيانات الخادم موضع الثّقة Compromise of DNS server's authoritative data

من التهديدات التي تواجه نظام أسماء النطاقات DNS هو حصول المهاجم علي صلاحيات عالية داخل نظام التشغيل (مثل صلاحية root داخل نظام unix) مما يمكنه من تعديل معلومات المجال zone area الخاصة بالملقم .
ويمكن التغلب علي هذا التهديد بتقليص الخدمات الموجودة علي الملقم الواحد وإعطاء الصلاحية للمديرين فقط وهذا هو المتبع بتطبيق BIND .

خامسا : حماية "نظام أسماء النطاقات" DNSSEC

قام مهندسي الإنترنت The Internet Engineering Task Force (IETF) بتشكّل لجنة عمل لتزويد نظام أسماء النطاقات DNS بالامتدادات الأمنيّة اللازمة لحماية النظام وعادة ما يطلق عليها إمتددات حماية نظام أسماء النطاقات DNSSEC extensions .هذه التّحسينات الأمنيّة إلى البروتوكول صممت لتكون قابلة لمعالجة الثغرات الغير مدركة داخل نظام أسماء النطاقات DNS .

ولزيادة الحماية فقد تم إستخدام نظام توثيق البيانات بإستخدام ما يسمي بالمفتاح العام والخاص Public and Private Key حيث يتم تشيفر البيانات بإستخدم المفتاح الخاص بالملقم ويقوم الجهاز الطرفي بالتاكد من صحة مصدر البيانات عن طريق المفتاح العام للملقم وبذلك يكون قد تم إنجاز خطوة هامة في حماية ودرجة وثوقية البيانات .

المراجع:

http://www.tech-faq.com/dns.shtml
http://www.boutell.com/newfaq/definitions/dns.html
http://www.rsc-northwest.ac.uk/technical/dns/The%20DNS.asp
http--www.sanog.org-sanog1-dnstrain.pdf
http://www.fistconference.org/data/presentaciones/dnssecurity.pdf
http://www.ep.net/training/tld-rio-day2.pdf
http://security.polito.it/doc/pub/dnssec.pdf
http://www.zytrax.com/books/dns/ch13/#security