المجلة الدولية للهندسة وتقنية المعلومات
journal homepage:www.ijeit.misuratau.edu.ly

دراسة استقصائية حول بروتوكول نظام اسم المجال والتحديات الأمنية المصاحبة له

وسام محمد الترجمان
جامعة مصراتة- كلية تقنية المعلومات، قسم علوم الحاسوب، مصراتة، ليبيا
w.attorjman@gmail.com

الملخص— **تكمن أهمية بروتوكول نظام اسم المجال في كونه أساسيا للقيام بأي عملية اتصال على شبكة المعلومات الدولية (الإنترنت)، مما يجعل خوادم هذا البروتوكول على الشبكة هدفا مهما لقراصنة المعلومات. وذلك لأن السيطرة على خادم نظام اسم المجال يعني السيطرة التامة على الشبكة التابعة له حيث يمكن من خلال ذلك الخادم توجيه اتصالات المستخدمين لأي خوادم وهمية للحصول على بياناتهم الخصوصية مثلا، أو قطع كافة الاتصالات عنهم. و على الرغم من أهمية هذا البروتوكول و حساسيته الأمنية إلا أن التصميم الأساسي له لم يأخذ بعين الاعتبار الاحتياطات الأمنية اللازمة لضمان عدم اختراق خوادم هذا البروتوكول و ذلك لأن أمن المعلومات لم يكن على قائمة الأولويات في ذلك الوقت من عمر شبكة الإنترنت.**

بعد تنفيذ البروتوكول والعمل به لعدة سنوات أظهرت الأبحاث المختلفة نقاط ضعف وثغرات أمنية متنوعة فيه. إذ يمكن تنفيذ العديد من الهجمات التخريبية عن طريق استغلال تلك الثغرات والتي من الممكن أن تشكل خطورة بالغة على كافة مستخدمي شبكة الإنترنت. وتركز الأبحاث الحديثة لأمن المعلومات على إنشاء إجراءات عملية مضادة للتغلب على تلك المشكلات.

ولكي نضع القارئ في السياق المناسب لمحتوى المقالة رأينا أن نسلط الضوء في البداية على أساسيات عمل البروتوكول ثم ننتقل للحديث عن الثغرات الأمنية الموجودة بتصميم البروتوكول، وأخيرا سنقوم باستعراض الطرق المتبعة حاليا للتغلب على تلك الثغرات.

الكلمات المفتاحية: **شبكات الاتصالات، الإنترنت، أمن البيانات DNS، DNSSEC**

1. المقدمة

نظام اسم المجال هو قاعدة بيانات موزعة عالميا تقوم بتخصيص عناوين إنترنت لأسماء مُستضيفي الخدمات على الشبكة. هذا النظام ما هو إلا امتداد لنظام سابق يعرف باسم (HOSTS.TXT) وهو عبارة عن ملفات نصية يتم الاحتفاظ بها على خادم الشبكة (SRI-NIC) ويتم توزيعها على جميع مُستضيفي الخدمات في الشبكة. ومع تزايد أعداد هؤلاء المستضيفين أصبحت تكلفة توزيع تلك الملفات كبيرة جدا مما خلق مشكلات في المرونة وقابلية التوسع، بالإضافة إلى أن التحكم المركزي في التحديث لا يتماشى مع الاتجاه نحو المزيد من الإدارة الموزعة للإنترنت [1].

يمكننا أن نتخيل بروتوكول نظام اسم المجال كقاعدة بيانات موزعة يتم تنفيذ الاستعلامات بها في تسلسل هرمي لخوادم البروتوكول، والتي يمكن لموزع خدمة الإنترنت الاتصال بها عن طريق المنفذ رقم 53 ببروتوكول حزم بيانات المستخدِم (UDB) وبالتالي الاستعلام عن العنوان المطلوب. وتوجد ثلاث فئات رئيسية من خوادم بروتوكول نظام اسم المجال هي: خوادم الجذر وخوادم المستوى العلوي والخوادم الموثوقة. تتعاون هذه الخوادم لتوفير خدمة ترجمة الاسم الوصفي وهو اسم يسهل تذكره مثل (google، Facebook، amazon) لمستضيف الخدمة إلى عنوان إنترنت وهو ما تستطيع الموجهات التي تعمل دخل الشبكة فهمه والعكس بالعكس.

استلمت الورقة بالكامل في 18 اغسطس 2020 وروجعت في 16 سبتمبر 2020 وقبلت للنشر في 18 سبتمبر 2020

ونشرت ومتاحة على الشبكة العنكبوتية في 17 اكتوبر 2020

بالإضافة إلى هذا فإن بروتوكول نظام اسم المجال يوفر خدمة الحصول على الاسم الرسمي وعنوان المستضيف عن طريق أي اسم مستعار لذلك المستضيف، وفيما يلي بعض الأمثلة على الأسماء المستعارة والرسمية.

المستعار الاسم	الرسمي الاسم
www.ibm.com	www.ibm.com.cs186.net
www.gmail.com	googlemail.l.google.com
mail.google.com	googlemail.l.google.com

كما أنه عادة ما يتم ربط أسماء المواقع المزدحمة بعدة خوادم لخلق توازن في أحمال الشبكة وكذلك لغرض تصحيح أخطاء التراسل. وبالطبع فإن لكل خادم عنوان إنترنت خاص به. وبالتالي يجب أن يكون لقاعدة بيانات البروتوكول القدرة على ربط مجموعة من عناوين الإنترنت باسم مستضيف أساسي واحد، فمثالا الاسم (googlemail.l.google.com) مربوط على الخادمين 74.125.225.118، 74.125.225.117. وعند الاستعلام عن اسم معين فإن البروتوكول يضمن الحصول على عناوين كل الخوادم المربوطة به. ولزيادة تحسين الأداء فإن البروتوكول يقوم بتدوير ترتيب عناوين الإنترنت في كل مرة يتم فيها الاستعلام عن نفس الاسم حتى يتسنى توزيع حركة مرور حزم البيانات داخل الشبكة على كل الخوادم. وتحتفظ خوادم البروتوكول بالبيانات فيما يعرف بسجلات الموارد والتي عادة ما تتكون من أربعة حقول هي: الاسم والقيمة والنوع ومدة الصلاحية. يحدد حقل مدة الصلاحية متى يجب إزالة سجل المورد من ذاكرة التخزين المؤقت بالخادم أما حقل النوع فيفسر حقلي الاسم والقيمة كما يلي:

- إذا كان النوع هو (A) فإن الاسم يمثل اسم المستضيف والقيمة هي عنوان الإنترنت لذلك المستضيف.
- إذا كان النوع هو (NS) فإن الاسم هو اسم النطاق والقيمة هي اسم مستضيف الخادم الموثوق والذي بدوره يعرف كيفية الحصول على عناوين مستضيفي هذا النطاق.
- إذا كان النوع هو (CNAME) فإن الاسم هو الاسم المستعار للمستضيف والقيمة تمثل الاسم الرسمي له.
- إذا كان النوع هو (MX) فإن الاسم هو الاسم المستعار للمستضيف والقيمة هي عنوان خادم البريد الإلكتروني المقابل لاسم المستضيف. يسمح هذا النوع للمؤسسة بالحصول على نفس الاسم المستعار لخادم البريد الخاص بها بالإضافة لأحد مستضيفيها العاملين مثل خادم الويب.

لا يوجد خادم واحد في التسلسل الهرمي لقاعدة بيانات اسم المجال يعرف كل المعلومات حول جميع مستضيفي الإنترنت، إنما يتم توزيع هذه المعلومات على ثلاثة مستويات من الخوادم.

المستوى الأول – الخوادم الجذرية. يوجد ثلاثة عشر خادما جذريا لأسماء مجالات الإنترنت تبدأ أسماؤها بالحروف اللاتينية من (a) إلى (m). هذه الخوادم مسؤولة عن تتبع عناوين خوادم المستوى التالي في التسلسل الهرمي. كل واحد من هذه الخوادم الثلاثة عشر هو في الواقع مجموعة من الخوادم المنسوخة ويعرض الشكل 1 عناوين الإنترنت لتلك الخوادم.

المستوى الثاني – خوادم النطاق العلوي. هذه الخوادم مسؤولة عن اسم نطاق المستوى الأعلى للمجال مثل (com.) و (edu.).

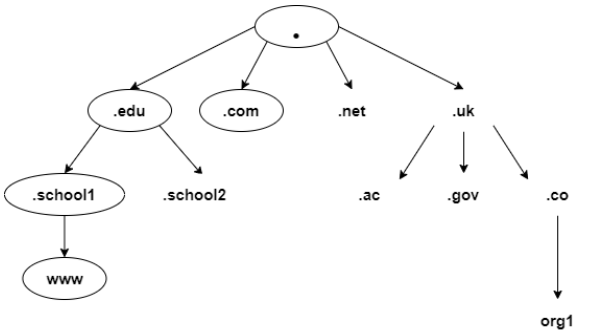
```
a.root-servers.net. 198.41.0.4
a.root-servers.net. 2001:503:ba3e::2:30
b.root-servers.net. 192.228.79.201
c.root-servers.net. 192.33.4.12
d.root-servers.net. 128.8.10.90
d.root-servers.net. 2001:500:2d::d
e.root-servers.net. 192.203.230.10
f.root-servers.net. 192.5.5.241
f.root-servers.net. 2001:500:2f::f
g.root-servers.net. 192.112.36.4
h.root-servers.net. 128.63.2.53
h.root-servers.net. 2001:500:1::803f:235
i.root-servers.net. 192.36.148.17
i.root-servers.net. 2001:7fe::53
j.root-servers.net. 192.58.128.30
j.root-servers.net. 2001:503:c27::2:30
k.root-servers.net. 193.0.14.129
k.root-servers.net. 2001:7fd::1
l.root-servers.net. 199.7.83.42
l.root-servers.net. 2001:500:3::42
m.root-servers.net. 202.12.27.33
m.root-servers.net. 2001:dc3::35
```

شكل 1. أسماء الخوادم الجذرية لبروتوكول نظام اسم المجال وعناوينها على شبكة الإنترنت

المستوى الثالث – خوادم المستخدمين. ليكون لأي مؤسسة خدمة أو خدمات خاصة بها على الإنترنت يجب أن تمتلك خادم اسم مجال موثوق يقوم بربط أسماء مستضيفي خدمات تلك المؤسسة بعناوين الإنترنت المخصصة لهم. يجب كذلك تسجيل عنوان الإنترنت لخادم اسم المجال الموثوق بأحد خوادم المستوى الأعلى. فمثلا لتسجيل اسم المجال (example.com) يجب تسجيل الخوادم الموثوقة الأساسية والثانوية لهذا المجال في أحد خوادم النطاق العلوي(com.). فإذا افترضنا أن الخوادم الموثوقة الأساسية والثانوية لهذا المجال هي (ns1.example.com) و (ns2.example.com) وأن عناوين الإنترنت الخاصة بهما هي 210.215.215.1، 210.215.215.2 على التوالي، فيجب أن يحتوي أحد خوادم النطاق العلوي (com.) على سجلات الموارد التالية.

الاسم	القيمة	النوع
example.com	ns1.example.com	NS
example.com	dns2.example.com	NS
dns1.example.com	210.215.215.1	A
dns2.example.com	210.215.215.2	A

مما سبق قد نستنتج أن خوادم النطاق العلوي تعرف جميع الخوادم الموثوقة في مجالها. قد يكون هذا صحيحًا في كثير من الحالات إلا أنه ليس صحيحًا بشكل عام، فعلى سبيل المثال إذا أخذنا المجال (org1.co.uk) في الشكل 2 نجد أن خادم النطاق العلوي (uk.) يعرف فقط خادم المجال الوسيط (co.) والذي بدوره يعرف عنوان الإنترنت للخادم (org1.).



شكل 2. مثال على التسلسل الهرمي لخوادم بروتوكول نظام اسم المجال.

قمنا في هذا الفصل بشرح مختصر لهيكلية ومكونات بروتوكول نظام اسم المجال. أما باقي هذه المقالة فقد تم ترتيبه على النحو التالي. في الفصل الثاني سنقوم بشرح آلية عمل بروتوكول نظام اسم المجال بشيء من التفصيل مع بعض الأمثلة التوضيحية، وفي الفصل الثالث سنقدم تصنيفا للتهديدات الأمنية التي يتعرض لها البروتوكول. أما الفصل الرابع فيشرح ملحق الأمان (DNSSEC) والذي يهدف لحل العديد من أوجه القصور الأمنية في البروتوكول موضوع الدراسة. في الفصل الخامس تم استعراض بعض أنوع عمليات القرصنة الشهيرة للبروتوكول مع مناقشة موجزة للتدابير والدفعات المضادة الممكنة حيالها. وأخيرا في الفصل السادس نختتم هذه المقالة بمناقشة الحالة الراهنة لتنفيذ تلك الدفاعات والعوائق التي تحول دون اعتمادها. كما نود أن ننوه إلى أن كل الأمثلة بهذه المقالة تستخدم خادم اسم المجال (BIND) مع نظم تشغيل أوبونتو.

2. كيفية عمل البروتوكول

العمليتان الرئيسيتان للبروتوكول هما: عملية الاستعلام وعملية صيانة المنطقة. في الحالات الاعتيادية يتم تنفيذ كلا هاتين العمليتين باستخدام بروتوكول حزم بيانات المستخدم على المنفذ 53 بحجم 512 بايت للحزمة الواحدة مع وجود خيار التنسيق بين أي اثنين من الخوادم على استخدام أحجام أكبر أو استخدام بروتوكول التحكم بالإرسال (TCP) [2].
لكل مجال ضمن التسلسل الهرمي لقاعدة بيانات اسم المجال العالمية مساحة تعرف بمنطقة اسم المجال وتمثل حدود صلاحيات مالكها. بناء على تلك الصلاحيات قد تتكون منطقة اسم المجال من مجال واحد فقط أو عدة مجالات بالإضافة إلى المجالات الفرعية. يتم وصف جميع المجالات الخاضعة لسلطة المنطقة في ملف بيانات خاص يعرف بملف المنطقة. وبحسب المواصفات القياسية [3] فإن ملف المنطقة يحتوي على ترجمة اسم المجال إلى خصائص يمكن استخدامها في أي من برمجيات خوادم اسم المجال مثل (BIND).

أ. أنواع خوادم اسم المجال

تنقسم خوادم اسم المجال وظيفيا إلى نوعين رئيسيين هما خادم الاسم الموثوق وخادم تحليل الاسم. وعلى الرغم من أن حزمة برمجيات خادم اسم المجال عادة ما تكون قادرة على القيام بكلتا الوظيفتين إلا أنه عمليا يتم فصلهما في أغلب الأحيان.

خادم الاسم الموثوق الرئيسي. يحصل هذا الخادم على بيانات المنطقة مباشرة من ملف المنطقة بعكس الخادم التابع الذي يحصل على بيانات المنطقة الخاصة به من خلال عملية نقل البيانات من الخادم الرئيسي. يتم تعريف ملفات المنطقة التابعة للخادم الرئيسي في برنامج (BIND) باستخدام مجموعة من جمل الخيارات في ملف تكوين خاص يسمى (name.conf) وتبين الشيفرة البرمجية التالية مثالًا لأحد سجلات خادم الاسم الرئيسي للمجال (example.com) بهذا الملف.

```
...
zone "example.com" in {
  type master; // master server
  file "master.example.com"; // name of the
                             // zone on file
                             // system with
RRs
};
...
```

خادم الاسم الموثوق التابع. تشترط مواصفات بروتوكول اسم المجال أن يكون هناك على الأقل خادمان لدعم أي مجال أو منطقة. ومن الممكن تشغيل خوادم أسماء رئيسية متعددة ولكن يجب نسخ ملفات أي منطقة يتم تغييرها إلى جميع تلك الخوادم وبالتالي فإن كل خادم يجب أن يتوقف مؤقتا عن العمل لإتمام عملية إعادة تحميل الملفات الجديدة مما قد يتسبب في انخفاض سرعة الخدمة. لحل هذه المشكلة والحفاظ على مستوى الخدمة يتم تخصيص خادم اسم رئيسي واحد للمنطقة وتكون الخوادم الأخرى تابعة له. حيث يتم تعريف المنطقة محليا على الخادم الرئيسي فقط بينما يتم توزيع أي تغييرات في بيانات المنطقة على جميع الخوادم التابعة من خلال عملية صيانة المنطقة والتي سيتم شرحها في الفصل 2.ب. وبالرغم من أن الخادم التابع يحصل على معلومات المنطقة من الخادم الرئيسي إلا أنه يستطيع الرد على الاستعلامات عن اسم المجال كما لو كان الخادم الرئيسي.

خادم تحليل الاسم. تتحصل خوادم التحليل على سجلات الموارد من خادم اسم المجال الموثوق عندما يتم الاستعلام عنها لأول مرة، وتقوم بتخزين تلك الإجابة محليًا بشكل مؤقت ليتم الرد لاحقا على الاستعلامات عن نفس المجال من ذاكرة التخزين المؤقت. ويعتمد انتهاء صلاحية البيانات المخزنة مؤقتًا على قيمة حقل مدة الصلاحية في سجل المورد. تساعد عملية التخزين المؤقت في رفع كفاءة أداء المستضيف المحلي بشكل كبير وذلك بتجنب الطلب المتكرر لسجلات الموارد من الخوادم الموثوقة على الشبكة. كما أنه يقلل بشكل كبير من ازدحام الشبكة.

عند الاستعلام عن بيانات غير متوفرة في ذاكرة التخزين المؤقت فإن هذا الخادم سيقوم بالبحث عن تلك البيانات بالخوادم الموثوقة بشكل عودي (recursive) للحصول على الإجابة. في برنامج (BIND) تحدد الخاصية (recursion) ضمنيا أن الخادم مسموح له بالتخزين المؤقت. ويوضح المثال التالي جزءا من ملف (name.conf) المستخدم لتعريف خادم اسم التخزين المؤقت ببرنامج (BIND). وكإجراء وقائي بسيط لإعاقة نجاح الاختراق الأمني المعروف بهجوم رفض الخدمة الموزع (DDoS) يتم تقييد العملاء الذين يمكنهم البحث العودي من خلال تحديد عناوين الإنترنت الخاصة بهم كما هو موضح في نفس المثال؛ فإذا وصل استعلام عودي من عنوان إنترنت غير محدد بالقائمة يتم رفضه.

```
...
options {
  recursion yes; // turns on caching behavior

  // define IPs that are allowed to issue
  // recursive queries
  allow-recursion {10.2/16;192.168.2/24;};
};
...
```

ب. صيانة المنطقة

يتم تعريف عنوان الإنترنت الخاص بالخادم الرئيسي في ملف (name.conf) للخادم التابع الذي يقوم بطلب بيانات المنطقة من الخادم الرئيسي بشكل دوري. زمن تكرار هذا الطلب يتحدد بواسطة معلمة التحديث في سجل مورد خاص يعرف بسجل نفوذ المنطقة الذي يتم تعريفه في بداية ملف بيانات المنطقة بالخادم الرئيسي. يحتوي هذا السجل على اسم الخادم الرئيسي وبعض المعلمات الخاصة بالمنطقة مثل معدل تحديث البيانات ووقت انتهاء الصلاحية والرقم التسلسلي [3]. تبدأ عملية نقل بيانات المنطقة من الخادم التابع وذلك بالاستعلام عن سجل نفوذ المنطقة من الخادم الرئيسي. إذا كان الرقم التسلسلي بسجل نفوذ المنطقة أكبر من رقم السجل الحالي الذي يحتفظ به الخادم التابع فإنه سيطلب من الخادم الرئيسي بيانات المنطقة بالكامل [4]. ولكن نقل كل بيانات المنطقة غالبا ما يتطلب نقل ملفات كبيرة الحجم وبالتالي سعة كبيرة على الشبكة والكثير من الوقت. فإذا كان التغيير الحاصل في بيانات المنطقة صغيرا فإن هذا الإجراء يكون مكلفا للغاية وغير عملي. لتجنب ذلك يقدم [5] أسلوبا آخر لتتم عملية نقل بيانات المنطقة بشكل تدريجي مما يتيح للخوادم إمكانية تبادل السجلات الحاصل بها تغيير فقط. إذا حدث فشل في عملية نقل بيانات المنطقة فإن الخادم التابع يستمر بتكرار الاستعلام بحسب الفترة الزمنية المحددة في سجل نفوذ المنطقة. أما إذا لم تنجح العملية قبل انتهاء صلاحية سجل نفوذ المنطقة الذي يحتفظ به الخادم التابع فإن هذا الخادم سيتوقف عن الاستجابة عن أي استفسارات أخرى عن هذه المنطقة إلى أن يحصل على سجل نفوذ جديد.

لاحظ أن الخادم التابع يجب أن ينتظر الوقت المحدد في معلمة التحديث في سجل نفوذ المنطقة قبل أن يبدأ بطلب تحديث بيانات المنطقة. وبالتالي فإن القيمة المعطاة لهذه المعلمة تتحكم بشكل أساسي في الوقت المستغرق لنشر أي تغييرات في بيانات المنطقة. وتوصي مواصفات البروتوكول بأن تتراوح هذه الفترة من ساعتين إلى اثنتي عشرة ساعة [6]. مما يعني أن التغييرات التي تطرأ على بيانات المنطقة قد لا تكون مرئية للخوادم التابعة إلا بعد مرور 12 ساعة على تغييرها. وللتغلب على هذه المشكلة يقترح المؤلف في [7] بأن يقوم الخادم الرئيسي للمنطقة بتعميم رسالة تنبيه لكل الخوادم التابعة بالمنطقة في كل مرة يتم فيها إعادة تحميل ملفات البيانات به وأن يبدأ الخادم التابع بطلب نقل بيانات المنطقة فور استلام تلك الرسالة.

إعادة تحميل ملفات بيانات المنطقة عادةً ما يؤدي إلى توقف الخادم عن العمل أثناء التحميل. ولكن مستضيفي الخدمات يريدون أن يتم تغيير سجلات المنطقة مع استمرار الخادم بالعمل والرد على الاستعلامات. لذلك يتم التحديث باتباع نظام يعرف بنظام تحديث اسم المجال الديناميكي [8]. القيد الوحيد على هذا النظام أنه لا يسمح بإضافة مجال أو منطقة جديدة أو حذفها بشكل ديناميكي. أي أنه يمكن تغيير جميع أنواع سجلات الموارد ما عدا سجل نفوذ المنطقة لأن تغييره يعني حذف منطقة وإضافة منطقة أخرى. في العديد من الحالات يوجد أكثر من خادم موثوق للمنطقة نفسها، ولضمان اتساق بيانات المنطقة يتم تنفيذ جميع أنواع التحديثات فقط على الخادم الموثوق الرئيسي وهو الخادم الذي يظهر في سجل نفوذ المنطقة.

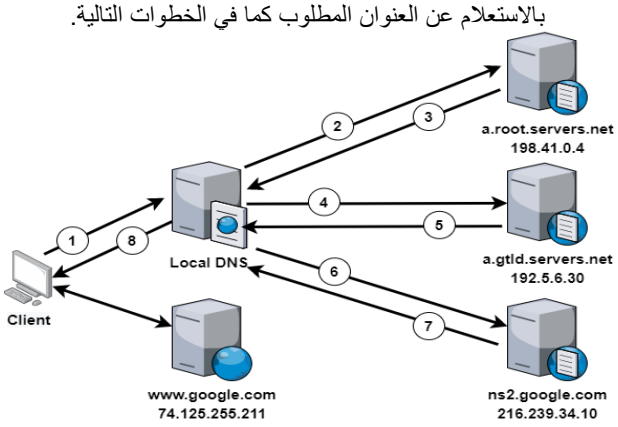
جـ. الاستعلام

تتمثل المهمة الرئيسية التي يقوم بها خادم الاسم موثوق في الإجابة عن الاستعلامات القادمة من خادم تحليل الاسم أو خادم اسم آخر يعمل بالنيابة عنه. فمزود خدمة الإنترنت يعطي عملائه عنوان أو عناوين الإنترنت لخوادم تحليل الاسم الخاصة به. ويتم ذلك في نظام لينوكس عادة عن طريق بروتوكول تكوين المستضيف الديناميكي حيث يُحفظ موقع خادم تحليل الاسم المحلي عادةً في ملف (resolve.conf). وعند وصول الاستعلام لخادم الاسم الموثوق للمجال فإنه قد يتولى المسؤولية الكاملة في البحث عن الإجابة وذلك بالبحث بشكل عودي في خوادم الأسماء الأخرى إلى أن يتم العثور على الإجابة النهائية، أو قد لا يجيب عن الاستعلام إلا إذا كان متعلقاً بمنطقته. وفيما يلي توضيح أكثر لهذين النوعين من الاستجابة.

استجابة الاستعلام العودية. يقوم الخادم بالعمل الضروري للإجابة الكاملة على الاستعلام. فإذا كانت الإجابة غير متوفرة عند الخادم فإنه يرسل استفسارات عودية إلى الخوادم الموثوقة الأخرى بناءً على تسلسلها الهرمي إلى أن يحصل على الإجابة. أي أن الخادم إما أن يرد على الاستعلام بعنوان المجال المطلوب أو بعلامة الخطأ (NXDOMAIN) والتي تشير إلى أن المجال المطلوب غير موجود أو علامة خطأ أخرى تشير لنوع آخر من الأخطاء الممكنة كحدوث فشل في الاتصال على الشبكة.

استجابة الاستعلام التكراري. هذه النوعية من الخوادم يمكنها فقط الرد على الاستعلام إذا كانت الإجابة متاحة محليًا. فيما عدا ذلك فإن هذا النوع من الخوادم سيحيل الاستعلام لخادم في المستوى التالي ولكنه لن يقوم باستفسارات إضافية نيابة عن العميل.

ولتوضيح كيفية عمل بروتوكول الاستعلام عن اسم المجال دعنا نلقي نظرة على مثال بسيط للاستعلام العودي. افترض أن جهاز العميل الذي يظهر في الشكل 3 يريد الحصول على عنوان الإنترنت الخاص بالمستضيف (www.google.com). بناء على ذلك فإن هذا العميل سيقوم بالاستعلام عن العنوان المطلوب كما في الخطوات التالية.



شكل 3. بروتوكول تبادل الرسائل بين خوادم اسم المجال

شكل 3. بروتوكول تبادل الرسائل بين خوادم اسم المجال.

1. يبدأ العميل بطلب الحصول على عنوان المستضيف (www.google.com) من خادم تحليل الاسم بالشبكة المحلية للعميل. إذا كانت الإجابة متوفرة في ذاكرة التخزين المؤقت للخادم المحلي فإنه سيقوم بالرد مباشرة على هذا الاستعلام وبذلك تنتهي العملية.
2. أما إذا لم تكن الإجابة متوفرة في ذاكرة التخزين المؤقت للخادم المحلي فإنه سيختار أحد الخوادم الجذرية بشكل عشوائي، ثم يقوم بإعادة توجيه الاستعلام إليه.

3. لا يعرف الخادم الجذري أي شيء عن المستضيف (www.google.com) لكنه سيرد بقائمة تحتوي على خوادم المستوى الأعلى المسؤولة عن المجال (com.) و تبين القائمة أدناه مثالًا على ذلك والتي حصلنا عليها بتوجيه الاستعلام للخادم (a.root.servers). في هذه القائمة قسم الصلاحيات (AUTHORITY) في تلك القائمة هو عبارة عن مجموعة من سجلات الموارد تسرد أسماء الخوادم ويعرض القسم الإضافي (ADDITIONAL) عناوين الإنترنت الخاصة بهم.

```
; <<>> DiG 9.8.1-P1 <<>> @a.root-servers.net www.google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16400
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 14
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.google.com.                IN      A

;; AUTHORITY SECTION:
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.

;; ADDITIONAL SECTION:
g.gtld-servers.net.     172800  IN      A       192.5.6.30
g.gtld-servers.net.     172800  IN      AAAA    2001:503:a83e::2:30
h.gtld-servers.net.     172800  IN      A       192.33.14.30
h.gtld-servers.net.     172800  IN      AAAA    2001:503:231d::2:30
b.gtld-servers.net.     172800  IN      A       192.26.92.30
f.gtld-servers.net.     172800  IN      A       192.31.80.30
i.gtld-servers.net.     172800  IN      A       192.12.94.30
a.gtld-servers.net.     172800  IN      A       192.35.51.30
l.gtld-servers.net.     172800  IN      A       192.42.93.30
n.gtld-servers.net.     172800  IN      A       192.54.112.30
j.gtld-servers.net.     172800  IN      A       192.43.172.30
e.gtld-servers.net.     172800  IN      A       192.48.79.30
d.gtld-servers.net.     172800  IN      A       192.52.178.30
k.gtld-servers.net.     172800  IN      A       192.41.162.30
m.gtld-servers.net.     172800  IN      A       192.55.83.30
c.gtld-servers.net.     172800  IN      A       192.26.92.30

;; Query time: 64 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Thu Sep 20 10:18:49 2012
;; MSG SIZE  rcvd: 504
```

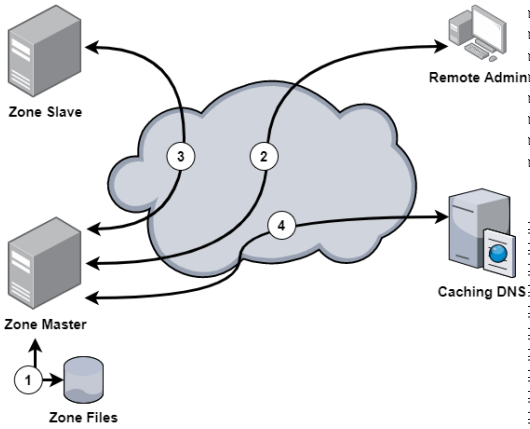
4. يختار خادم تحليل الاسم أحد خوادم المستوى الأعلى من تلك القائمة ويعيد إرسال نفس الاستعلام إليه.
5. ستتضمن إجابة خادم المستوى الأعلى قائمة بأسماء الخوادم الموثوقة للمجال (google.com) وعناوينها.
6. لقد كان من بين العناوين التي حصلنا عليها عند توجيه الاستعلام للخادم (a.gltd.servers) في الخطوة 5 هو عنوان الخادم ns2.google.c. مرة أخرى يرسل خادم تحليل الاسم نفس الاستعلام إلى أحد الخوادم الموثوقة للمجال المطلوب للحصول على الإجابة. لاحظ أن الإجابة في كل مرة عبارة عن مجموعة من سجلات الموارد.
7. وعند توجيه الاستعلام للخادم (ns2.google.c) فإنه سيرد بعنوان المستضيف (www.google.com).
8. أخيرًا يرسل خادم تحليل الاسم الإجابة التي تم الحصول عليها إلى العميل.

يجب أن يكون لكل استعلام صادر عن خادم الاسم عدد صحيح فريد (مكون من 16 بت) يسمى مُعرّف الاستعلام. ليتسنى فيما بعد ربط كل استعلام بالإجابة الخاصة به عن طريق مطابقة رقم منفذ بروتوكول حزم البيانات ورقم مُعرّف الاستعلام لكل من الاستعلام والإجابة. لاحظ أن خادم تحليل الاسم يستخدم دائمًا المنفذ رقم 53 للإرسال، لكن رقم منفذ الاستقبال غير محدد.

3. التهديدات الأمنية لبروتوكول اسم المجال

كونه العمود الفقري للإنترنت يعد بروتوكول اسم المجال هدفًا مغريًا لقراصنة المعلومات. وبالفعل فقد تم تنفيذ العديد من الهجمات في الماضي بدرجات متفاوتة من النجاح. يمكن أن تستهدف الهجمات البروتوكول في حد ذاته أو أن تستهدف حزمة برمجية معينة لتنفيذ البروتوكول. نهتم هنا بالنوع الأول من الهجمات بينما النوع الثاني يعتبر خارج نطاق هذه المقالة. إذا ما نجحت الهجمات المنفذة على بروتوكول اسم المجال يمكن أن تكون خطيرة جدًا. ولأن طريقة عمل البروتوكول غير مرئية مباشرة للمستخدم العادي في متصفحه أو هاتفه المحمول فلا يتم اكتشاف الهجمات بسهولة؛ على هذا البروتوكول من قبل المستخدمين العاديين. واعتمادًا على التسلسل الهرمي لخادم البروتوكول الذي تتم مهاجمته يمكن للمهاجم أن يؤثر على عدد كبيرا من المستضيفين بهجوم واحد مما يوفر له عائدا جيدا للجهد المبذول في تنفيذ الهجوم.

سنصنف في هذا الفصل أنواع الهجمات الممكنة على البروتوكول بناء على مكان حدوث الهجوم أثناء عمل البروتوكول، بينما أجلنا إعطاء أمثلة عنها حتى الفصل 5. يوضح الشكل 4 الصورة العامة للمكونات الرئيسية لنظام البروتوكول ومسارات الإجراءات الرئيسية به. في كل مسار، نطرح السؤال التالي: ما هي التهديدات الأمنية المحتملة في هذا المسار؟ وفيما يلي سنجيب باختصار عن هذه الأسئلة.



شكل 4. مسارات الإجراءات الرئيسية لبروتوكول اسم المجال.

1. مسار تحميل ملفات المنطقة. تحتوي ملفات المنطقة وملفات تكوين البروتوكول على الكثير من البيانات التي تهم المهاجم وبالتالي يجب حمايتها. الحماية النموذجية هنا تتمثل بوضع سياسة جيدة لإدارة النظام مثل محدودية الوصول إلى هذه الملفات. من بين الآليات المستخدمة على نطاق واسع لهذا الغرض حجب خادم البروتوكول الرئيسي خلف جدار حماية يسمح فقط للخوادم التابعة للمنطقة بالوصول إليه. ويتم فتح جدار الحماية فقط للسماح بنقل ملفات المنطقة من الخادم الرئيسي إلى الخوادم التابعة.

2. مسار التحديثات الديناميكية. أشرنا سابقا إلى أن آلية التحديث الديناميكي تُستخدم لتحديث ملفات المنطقة على الخادم الرئيسي. يمكن للمهاجمين استهداف هذه الآلية لحقن بعض التحديثات التي تخدم مصالحهم في اختراق النظام. مثل هذه التحديثات قد تؤدي إلى إتلاف ملفات المنطقة على الخادم الرئيسي مما يؤدي إلى عطب المنطقة بأكملها. لحماية النظام من هذا التهديد الخطير يجب استخدام قيود صارمة على عناوين الإنترنت المُصرح لها بإجراء التحديث أو تعطيل هذه الخاصية نهائيا والقيام بعملية التحديث يدويا. يوضح المثال التالي تكوينا لخادم اسم ببرنامج (BIND) يسمح فقط للعناوين 10.1.2.5 و 10.1.2.8 بتحديث المنطقة (example.com). إلا أن المهاجم يمكنه التغلب على ذلك بانتحال أحد العناوين المُصرح لها بالتحديث. لذلك فإن ملحق أمان بروتوكول اسم المجال والذي سنناقشه في الفصل التالي يوصي باستخدام تقنيات التشفير عند إجراء أي تحديثات ديناميكية.

```
...
options {
   ...
   allow-update {none;}; // none by default
   ...
};
...
zone "example.com" in{
   ....
   allow-update {10.1.2.5; 10.1.2.8};
   ....
};
...
```

3. مسار نقل المنطقة. تعد هذه العملية أيضا مصدرا رئيسيا للتهديدات. إذ يمكن للمهاجم أن يقوم بإفساد نظام أسماء المجالات في الخدام التابع إذا تمكن من خداعه وجعله يقبل تحديثات للمنطقة كان هو مصدرها. وكما في النقطة السابقة فإن أبسط طريقة لتأمين نقل المنطقة تكون باستخدام القيود على عناوين الإنترنت. ويوضح المثال التالي كيف يمكن تكوين البروتوكول على الخادم الرئيسي في برنامج (BIND) للسماح فقط لعناوين إنترنت محددة بطلب نقل المنطقة. بالمثل يمكن تهيئة الخادم التابع لقبول عمليات نقل المنطقة فقط من عناوين محددة. مرة أخرى لا يتغلب هذا النوع من الحماية على حيل انتحال عنوان الإنترنت ويوفر ملحق الأمان حلاً أفضلًا باستخدام تقنيات التشفير.

```
...
zone "example.com in{
   ...
   allow-transfer {10.1.2.5; 10.1.2.8};
   ...
};
...
```

4. مسار الاستفسارات. يمكن إفساد محتويات ذاكرة التخزين المؤقت بإعطاء إجابات خاطئة لخادم تحليل الاسم المحلي عند استعلامه عن أسماء المجالات [9]. هذه المشكلة لا يمكن التغلب عليها بالطرق التقليدية وإنما يمكن معالجتها فقط باستخدام ملحق الأمان. سنناقش هذه المشكلة بمزيد من التفصيل في الفصل 5 والفصل 4-ب.

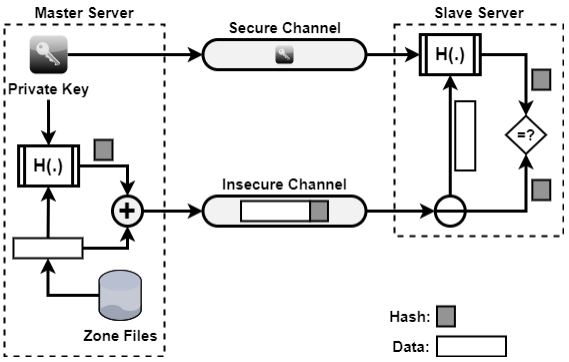
4. ملحق أمان بروتوكول اسم المجال (DNSSEC)

لقد تم تطوير ملحق أمان بروتوكول اسم المجال بهدف جعل البروتوكول أكثر أمانًا. وكما أوضحنا في الفصل السابق فإن بروتوكول اسم المجال يحتوي على العديد من نقاط الضعف التي تجعله عرضة للهجمات التخريبية على مستويات مختلفة. ويحاول ملحق الأمان معالجة تلك النقاط بالاستفادة من تقنيات تشفير البيانات. لعل أهم التحديات التي ستواجهنا هنا أن إخفاء البيانات ليس أحد أهداف بروتوكول اسم المجال. بل بالعكس فإن بيانات أسماء المجالات يجب أن تكون متاحة للجميع، إنما الهدف الرئيسي هو التأكد من عدم وجود تحديثات غير مصرح بها في تلك البيانات خلال تدفقها عبر المسارات المختلفة أثناء عمل البروتوكول. وبالتالي فإن المصادقة وتكامل البيانات هو ما يهمنا هنا وليس السرية. على أي حال عندما تكون السرية مطلوبة من الممكن توفيرها باستخدام أحد بروتوكولات الاتصال الآمن مثل SSL أو TLS. ويعتمد ملحق الأمان على مفهوم التشفير الحديث الذي يفترض أن كل الخوارزميات المستخدمة يجب أن تكون معروفة للجميع بما في ذلك المهاجم وأن الشيء السري الوحيد هو المفتاح المستخدم لتأمين الاتصال.

أ. تأمين نقل المنطقة

فكرة وضع القيود استنادا إلى عنوان الإنترنت الموضحة في الفصل السابق تفشل في حال تمكن المهاجم من انتحال أحد تلك العناوين، حيث يمكن للمهاجم انتحال عنوان الإنترنت الخاص بالخادم الرئيسي للمنطقة وعندها يمكنه نقل سجلات موارد تشير إلى مواقع ويب مختلفة (والتي يرغب هو بأن يوجه إليها المستخدمين) إلى الخوادم التابعة بالمنطقة. لذلك فإن تقنيات التشفير ضرورية لضمان مصادقة البيانات الرئيسية وتكامل بيانات المنطقة المنقولة. تم تعريف بروتوكول يسمى (TSIG) في [10] لتأمين نقل المنطقة باستخدام تقنيات التشفير. ويستخدم هذا البروتوكول تقنية التشفير المتماثل أي باستخدام مفتاح سري واحد مشترك بين الخادم الرئيسي والخادم التابع كجزء من رمز مصادقة الرسائل (MAC) كما هو موضح في شكل–5. حيث يقوم الخادم الرئيسي بعملية مزج بيانات المنطقة باستخدام المفتاح السري المشترك للحصول على رمز مصادقة الرسالة ثم يقوم بإلحاق ذلك الرمز ببيانات المنطقة ويرسله (بدون تشفير) إلى الخادم التابع. الخادم التابع الذي يستلم هذه الرسالة يبدأ أولا بفصل محتوى الرسالة عن رمز المصادقة ثم يعيد عملية المزج لمحتوى الرسالة باستخدام المفتاح المشترك وأخيرا يقارن الرمز الناتج مع الرمز المُستلَم ولا يقبل الخادم التابع البيانات إلا في حالة تطابق الرمزين. الآلية المستخدمة لتكوين وتبادل المفتاح المشترك بين الخادم الرئيسي والخوادم التابعة لم يتم تحديدها في [10] ولذا يجب الحفاظ على قناة آمنة أخرى لتبادل المفاتيح كبريد إلكتروني آمن مثلا. يحتوي برنامج (BIND) على أداة إضافية تُعرف باسم (dnssec-keygen) والتي يمكن استخدامها لإنشاء تلك المفاتيح. يجب إدراج المفتاح المشترك في ملف (name.conf) الخاص بالخادم الرئيسي والخادم التابع.

لاحظ أنه يمكن استخدام نفس البروتوكول لتأمين عملية التحديث الديناميكي كذلك. وعلى الرغم من أن هذا البروتوكول يستخدم تقنية تشفير قليلة التكلفة وهو مستخدم على نطاق واسع إلا أنه لا يخلو من بعض العيوب والتي من أهمها الحاجة لآلية اتصال خارجية بين الخوادم لمشاركة المفتاح الخاص بالتشفير. كما أن معظم برمجيات خوادم اسم المجال تتطلب إعادة التحميل كلما تم تغيير المفتاح الخاص بالتشفير نظرًا لضرورة تضمين هذا المفتاح في ملف (name.conf) مما يعني عدم إمكانية إجراء التحديث ديناميكيا على المفتاح السري المشترك.



شكل 5. آلية عمل بروتوكول.TSIG

للتغلب على أوجه القصور السابقة يمكن استخدام بروتوكول آخر يدعى (SIG0) معرف في [11] وهو يستخدم تقنية التشفير غير المتماثل للحفاظ على مصادقة المرسل وتكامل البيانات. تتميز تقنية التشفير غير المتماثل بوجود مفتاحين الأول يسمى المفتاح العام وهو ليس سري والثاني يسمى المفتاح الخاص وهو المفتاح السري. وبالتالي لا يلزم اتخاذ أي إجراء خاص لتوزيع المفاتيح العامة حيث يتم وضعها ببساطة في سجلات المفاتيح الرئيسية في ملف المنطقة ويمكن قراءتها من قبل أي شخص (بما فيهم المهاجم). لأن ما يجب أن يبقى سرياً الآن هو فقط المفتاح الخاص. ويعمل بروتوكول (SIG0) بشكل مماثل لبروتوكول (TSIG) غير أن العميل يستخدم المفتاح الخاص لإنشاء رمز المصادقة الذي يتم التحقق منه في الطرف المتلقي باستخدام المفتاح العام. وتستخدم سجلات موارد خاصة بهذا البروتوكول لإرسال رمز المصادقة والبيانات. ويتم إنشاء تلك السجلات ديناميكيًا بواسطة الخادم المرسل وتضاف إلى القسم الإضافي للبيانات المرسلة. ما أن تتم عملية التحقق حتى يقوم الخادم المستقبل مباشرة بإلغاء هذه السجلات؛ بمعنى أنه لا تتم إضافتها إلى ملف المنطقة. أداة (dnssec-keygen) يمكنها كذلك إنشاء المفاتيح العامة والخاصة المستخدمة في هذا البروتوكول. يبقى أن نشير إلى أن الجانب السلبي لتقنية التشفير غير المتماثل هو ارتفاع تكلفتها بالمقارنة مع تقنية التشفير المتماثل من حيث الزمن المطلوب للمعالجة.

ب. تأمين الاستعلامات

عندما يتلقى خادم الاسم الاستجابة عن أي استعلام يمكن فقط أن يأمل بأن تكون تلك البيانات صحيحة لعدم وجود طريقة لإثبات ذلك. ومن الممكن خداع ذلك الخادم بطرق متنوعة سنناقشها في الفصل التالي. ولكن التحديثات [12،13،14،15،16،17،18] على ملحق الأمان توفر العديد من المزايا الهامة باستخدام تقنيات التشفير المختلفة والتي من بينها اتاحة

وسيلة للخادم المستقبل للتحقق من أن الرسائل هي في الواقع من طرف مرسل مخول. حيث يمكن لخوادم الأسماء التي تم تكوينها لدعم ملحق الأمان التحقق من صحة وسلامة بيانات المنطقة المُتحصل عليها من استعلام مذيل بتوقيع رقمي. وتُستخدم تقنية التشفير غير المتماثل مع مجموعة خاصة من سجلات الموارد للقيام بما يلي:

- المصادقة – تُمكن التوقيعات الرقمية المشفرة خادم تحليل اسم المجال من التحقق من أن البيانات المستلمة قد صدرت من خادم الاسم الموثوق الخاص بالمنطقة المطلوبة.
- تكامل البيانات – يمكن لخادم تحليل اسم المجال التحقق من أن البيانات المستلمة من خادم الاسم الموثوق لم يتم العبث بها قبل وصولها.
- إثبات عدم وجود سجلات المورد – قد لا يوجد إجابة عن بعض الاستعلامات وبالتالي فإن خادم اسم المجال سيرد على تلك الاستعلامات بالرسالة الخاصة (NXDOMAIN) مشيرا لعدم وجود سجلات موارد متعلقة بالاستعلام. مثل هذه الإجابة قد يستخدمها المهاجم في تضليل خادم تحليل اسم المجال. ولكن ملحق الأمان يدعم آلية تتيح لخادم تحليل اسم المجال التحقق من أن مثل هذه الإجابة بعدم وجود سجلات موارد متعلقة بالاستعلام قد صدرت بالفعل من الخادم الموثوق لاسم المجال.

لكي يعمل ملحق الأمان بشكل صحيح يجب أن يكون كل من خادم اسم المجال وخادم تحليل اسم المجال معدّان لدعم الملحق. وذلك لأن خادم اسم المجال المزود بالملحق سيقوم بتوقيع ملف بيانات المنطقة رقميا لضمان نقطة دخول آمنة للنظام وبالتالي فإن كل الإجابات ستكون موقعة رقميا. لذا فإن هذا الخادم سيحتوي على سجلات الموارد الإضافية التالية:

- سجل مورد المفتاح (DNSKEY) يحتوي على مفتاح التشفير العام للمنطقة.
- سجل مورد التوقيع (RRSIG) يحتوي على التوقيع الرقمي لكل مجموعة مرتبطة من سجلات الموارد في ملف المنطقة.
- سجل مورد التأمين (NSEC) يحتوي على قائمة بجميع سجلات الموارد لكل مجال في ملف المنطقة. يتم استخدام هذه القائمة لإثبات عدم وجود أسماء مفقودة وبالتالي توفير خاصية إثبات عدم وجود سجلات موارد متعلقة بالاستعلام سابقة الذكر.

يتم توقيع ملفات المناطق رقميًا باستخدام مفتاح التشفير الخاص ويتم تخزين مفتاح التشفير العام المقابل لكل مفتاح خاص في سجل جديد من نوع سجل مورد المفتاح. يوجد نوعان من المفاتيح المستخدمة في عمليات توقيع المنطقة. النوع الأول يسمى مفتاح توقيع المنطقة (ZSK) والثاني يسمى مفتاح توقيع المفتاح (KSK). يستخدم مفتاح توقيع المنطقة لتوقيع مجموعات سجلات الموارد المرتبطة داخل المنطقة ويتضمن توقيع سجل مفتاح توقيع المنطقة نفسه. يتم تخزين التوقيع الرقمي لكل مجموعة مرتبطة من السجلات في سجل جديد من نوع سجل مورد التوقيع. يتم فقط توقيع سجلات الموارد التابعة للمنطقة نفسها. على سبيل المثال سجل مورد التفويض بالتوقيع لا يتم توقيعه لأنه ينتمي للمنطقة الفرعية.

أما مفتاح توقيع المفتاح فيستخدم لتوقيع المفاتيح فقط؛ أي أنه يستخدم لتوقيع كل من مفتاح توقيع المنطقة ومفتاح توقيع المفتاح التابعين للمنطقة. ويمكن تلخيص عملية توقيع المنطقة في الخطوات التالية:

1. يتم ترتيب جميع سجلات الموارد (غالبًا ما يكون أبجديًا استنادًا إلى اسم المضيف).
2. تتم إضافة سجل جديد من نوع سجل مورد التأمين بين كل اسمين للمجال في المنطقة لتحديد سجلات الموارد الموجودة في هذا المجال وللإشارة لاسم المجال التالي في المنطقة. يُعتبر كل سجل مورد تأمين بمثابة مجموعة سجلات مرتبطة، ويشير سجل مورد التأمين الأخير إلى جذر المنطقة.
3. يستخدم مفتاح توقيع المنطقة للتوقيع على كل مجموعة سجلات مرتبطة ومن ثم إنشاء سجل جديد من نوع سجل مورد التوقيع.
4. يستخدم مفتاح توقيع المفتاح لتوقيع سجلات مورد المفتاح.

جـ. *التعامل مع المناطق المختلطة*

يُسمى المجال مجالا آمنا إذا كان الخادم الموثوق لهذا المجال يستخدم ملحق الأمان. ونظرا للعدد الكبير من خوادم اسم المجال الموجودة على الإنترنت فإن اعتماد ملحق الأمان من قبل جميع الخوادم قد يستغرق وقتا كبيرا. أثناء ذلك يجب أن يعمل بروتوكول اسم المجال مع كل من المجالات الآمنة وغير الآمنة. تظهر مثل هذه الحالة في الشكل-2، حيث أن المجالات المحاطة بحلقة هي مجالات آمنة بينما المجالات الأخرى ليست كذلك. لنفترض أن هناك خادمي تحليل اسم مجال هما (ns1) و (ns2). الخادم (ns1) عبارة عن خادم تحليل داعم لملحق الأمان بينما (ns2) هو خادم تحليل عادي. أي استعلام يرسله الخادم (ns1) لخادم اسم مجال موثوق سيشمل علامة الأمان بسجلات الموارد في القسم الإضافي من الاستعلام. إذا كان الخادم الموثوق (على سبيل المثال: school1.edu) يدعم ملحق الأمان فإنه يستجيب للخادم (ns1) بمعلومات أمان إضافية على النحو المحدد في بروتوكول ملحق الأمان. نفس الخادم الموثوق إذا ما تلقى استعلامًا من (ns2) يلاحظ أنه لا توجد علامة أمان في القسم الإضافي فيرد على الاستعلام بالإجابة التقليدية.

د. *سلاسل الثقة*

يعتمد التشفير غير المتماثل كما نعلم على زوج من المفاتيح هما: المفتاح العام والمفتاح الخاص. ويجب على المُستقبل التحقق من أن المفتاح العام ينتمي للمُرسل الصحيح. في ملحق الأمان يتم ذلك باستخدام نقاط ربط موثوقة. دعنا نقول إن المنطقة (school1.edu) في الشكل-2 تم توقيعها بشفرة رقمية ما. يمكن لخادم التحليل (ns1) التحقق من التوقيع باستخدام المفتاح العمومي الخاص بـ (school1.edu) ولكن (ns1) يحتاج للتأكد من أن هذا المفتاح هو المفتاح الحقيقي. لنفترض أن (ns1) لديه رابط موثوق به للوصول إلى الخادم (school1.edu)، هذا يعني أنه بإمكان (ns1) استخدام هذا الرابط للتحقق من صحة المفتاح العمومي لـ (school1.edu). ولكن إنشاء رابط موثوق به في كل خادم تحليل لجميع المجالات الآمنة عبر الإنترنت ليس خيارا عمليا، ولهذا جاءت فكرة سلاسل الثقة.

يتم إنشاء سلاسل الثقة من خلال عملية التفويض، حيث يتم منح تفويض الثقة من المنطقة الأصل إلى المنطقة التابعة لها باستخدام سجل مورد خاص يعرف باسم سجل مورد التفويض (DS RR). تحتوي المنطقة الأصل على سجل مورد تفويض يحدد مفتاح توقيع المفتاح للمنطقة التابعة. أي خادم تحليل يثق بالمنطقة الأصل يمكنه الآن الوثوق بالمنطقة التابعة. يتم تكوين جميع خوادم التحليل لتثق في مفتاح توقيع المفتاح للمنطقة الجذر بشكل ثابت، لذلك تبدأ كل سلاسل الثقة عند المنطقة الجذر. لنفترض على سبيل المثال أن خادم تحليل يبحث عن سجل المورد من نوع (A) الخاص بخادم الوب (www.school1.edu) وليس لديه رابط موثوق لخادم اسم المجال (school1.edu). يمكن لهذا الخادم الآن أن يستخدم مفتاح توقيع المفتاح للمنطقة الجذر للتحقق من صحة مفتاح توقيع المنطقة، ثم أن يستخدم المفتاح الأخير للتحقق من صحة سجل مورد التفويض ومفتاح توقيع المفتاح للتحقق من مفتاح توقيع المنطقة للمنطقة التابعة (edu.)، ثم أن يستخدم مفتاح توقيع المنطقة (edu.) للتحقق من صحة سجل مورد التفويض ومفتاح توقيع المفتاح للتحقق من مفتاح توقيع المنطقة للمنطقة التابعة (school1.edu)، وأخيرًا يستخدم مفتاح توقيع المنطقة (school1.edu) للتحقق من سجلات المورد من نوع (A) الخاصة بخادم الوب (www.school1.edu). تُسمى هذه العملية سلسلة الثقة، ويمكن أن يغطي الرابط الموثوق للمنطقة الأصل أي مناطق آمنة تابعة له يتم تفويضها من قبله.

هـ. *المشاكل المصاحبة لملحق الأمان*

يذكر تقرير ICANN أن 30٪ فقط من خوادم النطاق العلوي المتصلة بخوادم منطقة الجذر تحتوي سجلات موقعة رقميا [19]. وبحسب الدراسة [20] على ملحق الأمان، فإنه حتى سنة 2013 يوجد مائة خادم من خوادم اسم المجال لأكبر مواقع التجارة الإلكترونية لا تنفذ توصيات ملحق الأمان بالكامل. وبالرغم من أن هذا العدد يعتبر كبيرا إلا أن المؤشرات كانت مطمئنة إلى حد ما حيث أن عملية تضمين ملحق الأمان بخوادم اسم المجال المختلفة على الشبكة كانت في تزايد وإن كان بسيطا. إلا أن هذا التزايد مع الأسف لم يستمر، حيث بينت الإحصاءات الحديثة بأن معدل استخدام ملحق الأمان على خوادم البروتوكول بالشبكة قد انحدار من 86% في سنة 2013 ليصل حتى 68% في سنة 2019 [21]. وقد يرجع ذلك لأن ملحق الأمان يضيف الكثير من التكلفة لتأمين معاملات بروتوكول اسم المجال. حيث أن أداء البروتوكول مع وجود ملحق الأمان يكون منخفضا إلى حد كبير، ليس فقط بسبب زيادة السعة اللازمة لتمرير سجلات الموارد الإضافية، ولكن أيضا بسبب طلب عمليات أخرى كسلاسل الثقة مثلا. أضف إلى ذلك أن العديد من الطرق التي تم استخدامها لتحسين أداء

البروتوكول قد لا تعمل في وجود ملحق الأمان. على سبيل المثال، أظهر [22] أن ملحق الأمان يضيف تكاليف كبيرة إلى عملية تحليل اسم المجال حيث وضح الباحث باستخدام برنامج محاكاة أنه عند استخدام ميزة الجلب المسبق لأسماء المجالات في وجود ملحق الأمان ينخفض أداء البروتوكول بشكل ملحوظ. بسبب هذه الأنواع من مشاكل الأداء والمشاكل الأخرى المتعلقة بالبنية الأساسية لا يزال ملحق الأمان غير منتشر بشكل كامل. ولأن ملحق الأمان يعتمد على سلسلة الثقة فلا يمكن للخوادم الموثوقة ذات المستوى الأدنى الاستفادة من ملحق الأمان حتى إذا كانت سجلاتها موقعة وذلك لانقطاع سلسلة الثقة عند خوادم النطاق العلوي. كما أن معظم الشركات حاليا تخصص ميزانيات كبيرة للصيانة الدورية اللازمة لضمان استمرار عمل بروتوكول نظام اسم المجال وغالبا ما يكون الحصول على تمويل إضافي للقيام بالترقية اللازمة لتنفيذ ملحق الأمان صعبا خاصة في وجود ضرورة للإنفاق على تحسينات أخرى مثل ترقية بروتوكول عنونة الأنترنت وترقية البنية التحتية للاتصالات المتنقلة وغيرها. ومن بين التحديات الأخرى التي تواجه عملية الترقية لاعتماد ملحق الأمان هو أن التوسع السريع للإنترنت لم يسمح بوجود خوادم احتياطية لتشغيل البروتوكول على الإنترنت، مما يعني وجود مخاطرة في إخراج أي خادم من الخدمة أثناء الترقية. كما تجدر بنا الإشارة لوجود مشكلات سياسية تؤدي لتأخير تبني الترقيات [9].

ولعل أنجح الإجراءات للدفع باتجاه انتشار تطبيق دفاعات تأمين خوادم بروتوكول نظام اسم المجال يتمثل في الإجراءات التشريعية وليس التقنية. على سبيل المثال، أدت القوانين التي تفرض على المؤسسات الكبرى الحصول على شهادات معتمدة لطبقة المقابس الآمنة (SSL) إلى إجبار تلك المؤسسات على تبني العديد من حلول الأمان المتعلقة بالبروتوكول. كما أن وضع تواريخ محددة بخوادم أسماء المجالات التي تدعم ملحق الأمان لرفض الاستجابة للخوادم الأخرى غير الداعمة لملحق الأمان من شأنه أن يجبر تلك الأخيرة على اعتماد ملحق الأمان. وكذلك تقديم خصومات من قيمة الترقيات الإلزامية المتعلقة بتأمين البروتوكول، ودعم برمجيات المصادر المفتوحة لخوادم البروتوكول، ورفع مستوى الوعي العام لدى المستخدمين من خلال تعريفهم بخطورة الهجمات على بروتوكول نظام اسم المجال والحاجة إلى اعتماد تحسينات الأمان المتعلقة به، تعد محركات أساسية لسرعة انتشار وتطبيق تحسينات الأمان وخلق تنافس بين الشركات والمؤسسات في سرعة تطبيق تلك التحسينات لاستقطاب الزبائن.

5. مهاجمة بروتوكول نظام اسم المجال

في هذا الفصل سنستعرض ثلاثة أنواع من الهجمات الشائعة على بروتوكول نظام اسم المجال. سنبدأ أولا بهجوم تسميم ذاكرة التخزين المؤقت، وهو هجوم على البروتوكول نفسه. أما الهجوم الأخير فليس هجوما مباشرا على البروتوكول وإنما يعتمد على استغلال البروتوكول للقيام بنوع آخر من الهجمات.

أ. هجوم تسميم ذاكرة التخزين المؤقت

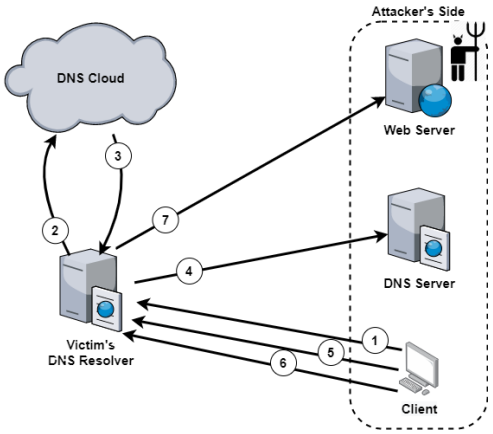
يهدف هذا الهجوم لتخريب الوظائف الأساسية لخادم تحليل اسم المجال مما يسبب عدم الثقة في البيانات الأساسية المخزنة بهذا الخادم والمتمثلة في ربط اسم المستضيف بعنوان الإنترنت الخاص به. وتعتمد فكرة عمل هذا الهجوم على أن خادم التحليل يتحقق من صحة الإجابة القادمة عن أي استفسار بالتأكد من:

1. رقم منفذ بروتوكول حزم بيانات المُستخدِم الذي تم استقبال الإجابة عليه.
2. رقم مُعرّف الاستعلام.
3. قسم السؤال والذي تنص مواصفات البروتوكول على وجوب تكراره في الرد على الاستفسارات.
4. وأخيرا ما يعرف باختبار منطقة النفوذ حيث يجب أن يكون اسم المجال موضوع الاستفسار ضمن نطاق منطقة نفوذ الخادم الذي قام بالرد.

إذا تم التأكد من صحة البيانات السابقة فإن خادم التحليل سيعتبر الإجابة صحيحة ويتم استخدامها وكذلك تخزين جميع أقسامها في ذاكرة التخزين المؤقت للخادم.

يُسمم هذا الهجوم ذاكرة التخزين المؤقت لخادم التحليل بحقنه بإجابات مزورة. حيث يمكن تنفيذ الهجوم إما بالتنصت على شبكة مزود خدمة إنترنت واعتراض استعلام صادر عن خادم التحليل التابع لها ثم محاولة تزوير إجابة للرد على ذلك الاستعلام، أو بإغراق خادم التحليل بإجابات خاطئة عن استعلام يقوم المهاجم بإرساله للخادم الضحية. ويعد النوع الثاني من هذا الهجوم أكثر خطورة من النوع الأول وذلك لأن المهاجم هو من يصنع استعلام التسميم وبالتالي يستطيع التحكم بمساحة تأثير هذا التسميم. وفيما يلي شرح مبسط لكيفية تنفيذ الهجوم.

لنفترض أن مُعرّف الاستعلام يزداد بواحد لكل استعلام صادر عن خادم التحليل. يمكن الآن إطلاق هجوم تسميم ذاكرة التخزين المؤقت كما هو موضح في الشكل 6 باتباع الخطوات التالية:



شكل 6. خطوات هجوم تسميم ذاكرة التخزين المؤقت.

1. يطلب المهاجم من خادم التحليل الضحية البحث عن مستضيف الخدمة التابع لنطاق المهاجم وليكن (www.attacker.com). يمكن للمهاجم هنا إرسال الاستعلام بنفسه إذا كان مسموحًا له بذلك، أو قد يتسلل لجهاز أحد مستخدمي شبكة الخادم الضحية ويقوم بإرسال الاستعلام منه.
2. يبدأ الخادم الضحية بجولة الاستعلامات حسب البروتوكول للحصول على عنوان الموقع (www.attacker.com).
3. في نهاية المطاف سيتم توجيه الخادم الضحية إلى عنوان الخادم (ns.attacker) الخاص بالمهاجم.
4. يمكن للمهاجم من خلال استعراض حركة عناوين الإنترنت بجهازه اكتشاف رقم منفذ بروتوكول حزم بيانات المُستخدِم و رقم مُعرّف الاستعلام اللذان استخدمهما الخادم الضحية للاستعلام.
5. يرسل المهاجم استعلام للخادم الضحية عن عنوان المضيف الذي يريد قرصنته، على سبيل المثال (www.foo.com).
6. لأن المهاجم يعلم بأن الخادم الضحية سيطلب من خادم اسم المجال (ns.foo.com) عنوان المضيف (www.foo.com)، فإنه يبدأ بإغراق الضحية بردود مزورة للعنوان (وهي عبارة عن سجلات موارد من نوع A تحتوي العنوان المزور). لاحظ أن المهاجم يمتلك كل البيانات المطلوبة لتزوير الرد. فقد تحصل على رقم المنفذ ورقم مُعرّف الاستعلام الأخير لخادم التحليل الضحية. أما قسم السؤال ومنطقة نفوذ المجال (ns.foo.com) فهي معلومات متوفرة للمهاجم من البداية.
7. إذا تطابق مُعرّف الاستعلام برد المهاجم مع مُعرّف الاستعلام المتوقع من قِبل الخادم الضحية قبل أن تصله الإجابة من موقع (ns.foo.com) الحقيقي، فسيتم قبول الإجابة المزورة كرد حقيقي بينما يتم تجاهل الإجابة الصحيحة المتأخرة.

تعتمد فكرة هذا الهجوم على أن أول إجابة جيدة تفوز وأن فرص إجابة المهاجم بالوصول قبل الرد الحقيقي أكبر. فإذا علم المهاجم (في الخطوة 4) أن رقم مُعرّف الاستعلام الحالي هو 999 مثلا فإنه سيرسل الردود المزورة برقم مُعرّف بدءًا من 1000 وبزيادة واحد لكل إجابة في محاولة للحصول على رقم مُعرّف مطابق للرقم المتوقع من طرف الخادم الضحية، أما إذا كان عنوان الموقع (www.foo.com) موجودًا في ذاكرة التخزين المؤقت للخادم الضحية فيجب على المهاجم الانتظار حتى انتهاء صلاحيته. أول إجراء احترازي يمكن اتخاذه حيال هذا الهجوم هو توليد رقم مُعرّف عشوائي لكل استعلام جديد بدلاً من زيادة الرقم بواحد في كل مرة. ولأن حجم حقل رقم مُعرّف الاستعلام هو 16 بت فإن المهاجم سيحتاج إلى 2^8 محاولة في المتوسط للحصول على رقم مطابق [23].

في المثال السابق، كان هدف المهاجم هو تسميم الإجابة النهائية، أي سجل المورد نوع A، ولكن دان كامينسكي [24] بين أن المجال بأكمله يمكن تلويثه بتسميم سجلات موارد منطقة النفوذ والأقسام الإضافية للإجابة، ويعمل الهجوم على النحو التالي:

1. أولاً يحتاج المهاجم إلى تكوين خادم اسم موثوق بنطاق (foo.com).
2. إرسال استعلام لاسم عشوائي من غير المرجح أن يكون في ذاكرة التخزين المؤقت مثل (agh571.foo.com).
3. كما في السابق سيستهدف المهاجم خادم تحليل اسم المجال للضحية، ولكن بدلاً من إعطاء إجابة نهائية بسجل مورد نوع (A) يحتوي على عنوان الإنترنت سيقوم المهاجم بتفويض خادم اسم آخر عبر سجلات منطقة النفوذ والأقسام الإضافية.
4. يحتوي سجل منطقة النفوذ على المجال الصحيح وهو (foo.com)، لذا فإن اختبار منطقة النفوذ سيمر بالرغم من أن القسم الإضافي يشير إلى خادم اسم المجال الخاص بالمهاجم.

في حال ما فشل المهاجم في الخطوة 3 (أي أن الإجابة الحقيقية كانت أسرع) فقد يبدأ جولة جديدة بإرسال استعلام آخر باسم مضيف عشوائي مختلف. بحسب [25] فإنه يمكن تحقيق النجاح في الغالب خلال 10 ثوانٍ. لذا فإن هذا الهجوم يعد خطيرًا للغاية لأن خادم تحليل اسم المجال للضحية يعتقد الآن أن خادم الاسم التابع للمهاجم هو الخادم الموثوق للمجال (foo.com).

إن الحجم الصغير (16 بت) لحقل رقم مُعرّف الاستعلام هو ما يجعل هذا الهجوم سهلًا. وبالتالي يمكن زيادة مساحة البحث عند المهاجم إلى 32 بت بجعل رقم منفذ بروتوكول حزم بيانات المُستخدِم عشوائيا كذلك، مما يعني أن متوسط عدد المحاولات الآن هو 2^{16}. على الرغم من أن هذا الحل قد يقلل من فرصة نجاح المهاجم، إلا أنه لا يمكن اعتباره حلاً نهائيًا خاصةً إذا أخذنا في الاعتبار النمو السريع في التقنيات الحاسوبية والسعات المتاحة بالشبكات. ولقد ناقش برديسي بعض المشكلات التي يتضمنها هذا الحل [9] خصوصا إذا ما كانت تقنية مترجم عنوان الشبكة (NAT) مستخدمة في شبكة الضحية وهي في الواقع تقنية مستخدمة بشكل كبير جدا عند مزودي الخدمة اليوم. وتتمثل صعوبة تنفيذ هذا الحل في وجود هذه التقنية في أن مترجم عنوان الشبكة قد يقوم بترجمة منفذ بروتوكول حزم بيانات المُستخدِم دون الحفاظ على العشوائية. وبالتالي فإن زيادة مساحة البحث من 16 بت إلى 32 بت تؤدي فقط إلى تقليل فرصة المهاجم للفوز بالسباق، ولكن لا يوجد أي ضمان لتكامل الاستعلام أو مصادقة الإجابة. إضافة لذلك لا يزال البروتوكول عرضة للعديد من الهجمات الأخرى كالتنصت على الشبكة، لهذا يوصي [23] بضرورة استخدام ملحق الأمان.

نظرًا لطبيعة ذاكرة التخزين المؤقت لخوادم التحليل فقد يستغرق الأمر وقتًا طويلاً حتى يتم اكتشاف وحذف كل المجالات المسممة والمحفوظة بالنظام، حيث تبقى سجلات الموارد المخزنة مؤقتًا في الذاكرة حتى انتهاء مدة الصلاحية. في [26] تم اكتشاف هجوم يمكن من إطالة عمر المجالات المسممة حتى بعد إزالتها من خوادم النطاق العلوي لبروتوكول نظام اسم المجال. ويمكن استخدام الهجوم نفسه للحفاظ على إدخالات ذاكرة التخزين المؤقت المسمومة لفترة طويلة دون الحاجة إلى شن هجوم تسميم الذاكرة مرة أخرى.

التسلل بين أجهزة الشبكة. في شبكات البيانات التي تعمل بدون مبدلات لا يحتاج المهاجم لكثير من الجهد لتزوير هويته أو للتنصت على أجهزة المستخدمين الآخرين فبوضع بطاقة الشبكة في وضع خاص يسمى الوضع المختلط يتم استلام كل حركة المرور بالشبكة بغض النظر عن عنوان الوسائط للوجهة. ومن ثم يمكن استكشاف حركة المرور باستخدام أي من برمجيات قراءة حزم البيانات كبرنامج (wireshark). إلا أن التنصت أو التسلل قد لا يكون سهلا في الشبكات التي تعمل بالمبدلات وذلك لأن المبدلات تقوم بتوجيه حزم البيانات للأجهزة حسب عنوان الوسائط الخاص بكل جهاز. ومع ذلك يوجد عدة تقنيات للالتفاف على هذا العائق ومن ثم الحصول على عدة ثغرات [27]. أحد أكثر الأساليب شيوعًا هو تسميم بروتوكول تحليل العنوان والذي سنقوم بتوضيح فكرة عمله فيما يلي.

في بيئة الشبكة التي تعمل بالمبدلات تحتفظ وحدة تحليل العنوان في كل جهاز بجدول للعناوين يخصص عناوين الإنترنت المقابلة لعناوين الوسائط الخاصة بالأجهزة الأخرى في الشبكة. يحتوي كل صف من جدول العناوين على الحقول التالية: عنوان الإنترنت و عنوان الوسائط المقابل له و زمن الصلاحية. إذا أراد الحاسوب A إرسال بيانات للحاسوب B فإن وحدة تحليل العنوان بالحاسوب A يمكن أن تحدد عنوان الوسائط للحاسوب B من عنوان الإنترنت للحاسوب B. الحاسوب A يمكنه الآن إنشاء حزمة بيانات في إطار طبقة ربط الوسائط بعنوان الوسائط للحاسوب B كعنوان للوجهة وإرسال تلك الحزمة عبر الشبكة. إذا لم يحتوي جدول العناوين بالحاسوب A على عنوان الحاسوب B فإن A سيقوم ببث حزمة استعلام عن عنوان الوسائط تحتوي على عنوان الإنترنت للحاسوب B. جميع الأجهزة على الشبكة ستتلقى حزمة استعلام ولكن فقط B من يرد بإرسال عنوان الوسائط الخاص به. يقوم A بتحديث جدول العناوين الخاص به بناء على هذا الرد دون المصادقة على أن مصدر الحزمة المستلمة كان فعلا B. يمكن للمهاجم استغلال هذه الثغرة وذلك بإرسال رد مزور على حزمة الاستعلام المعممة من الحاسوب A تحتوي على عنوان الحاسوب M الذي هو تحت سيطرة المهاجم. لاحظ الآن أن الحاسوب A يقوم بتوجيه كل البيانات التي يرغب بإرسالها للحاسوب B إلى الحاسوب M. وباتباع نفس الخطوات السابقة مع الحاسوب B يمكن جعله كذلك يعتقد بأن الحاسوب M هو الحاسوب A. وهكذا يكون المهاجم قد تمكن من التسلل بين A، B وأصبح قادرًا على التنصت على كل البيانات المتبادلة بينهما وكذلك انتحال هوية كل منهما بالنسبة للآخر. يمكن استخدام هجوم تسميم بروتوكول تحليل العنوان كآلية للتنصت في شبكات البيانات، والتي يمكن استخدامها فيما بعد للقيام بهجوم تسميم ذاكرة التخزين المؤقت لبروتوكول اسم المجال.

تجدر بنا الإشارة هنا إلى وجه التشابه في التقنية الأساسية التي يستخدمها المهاجم والمدافع في هجوم تسميم بروتوكول تحليل العنوان وهجوم تسميم ذاكرة التخزين المؤقت لبروتوكول اسم المجال. كلا الهجومين يستند على تزوير العنوان في الرد ويكمن حل كلا الهجومين في مصادقة مُرسل الرد. إلا أن هجوم تسميم بروتوكول تحليل العنوان يعمل في نطاق عنوان الوسائط فقط بينما يعمل هجوم تسميم ذاكرة التخزين المؤقت في طبقة بروتوكول نظام اسم المجال على مستوى عناوين الإنترنت. كما يتطلب هجوم تسميم ذاكرة التخزين المؤقت أن تصل إجابة المهاجم قبل الإجابة الصحيحة ولا يوجد مثل هذا الشرط في هجوم تسميم بروتوكول تحليل العنوان.

ب. هجوم إعادة ربط اسم المجال

يستهدف هذا الهجوم مستعرض ويب الضحية ويتحصل المهاجم بواسطته على الامتيازات التالية:

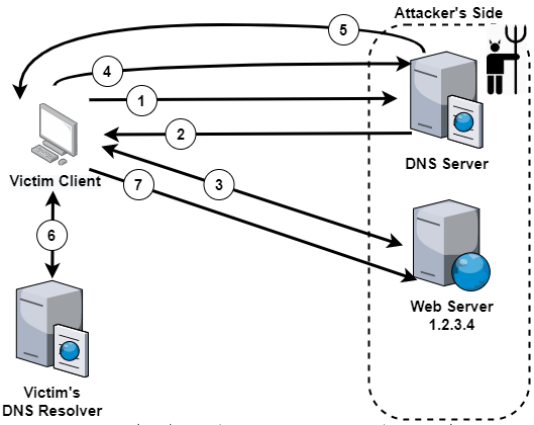
1. الوصول للمستضيفين الداخليين لشبكة الضحية والتي لا يمكن الوصول إليها من الإنترنت.
2. إعطاء جهاز المهاجم نفس امتيازات جهاز الضحية مما يسمح له بالوصول إلى موارد الشبكة التي تثق بالضحية.
3. انتحال شخصية الضحية وتنفيذ المزيد من الهجمات أو الأنشطة غير القانونية الأخرى مثل نشر البريد الإلكتروني المؤذي (spam email).

تقوم معظم المتصفحات باتباع ما يعرف بسياسة نفس المصدر. وتتبنى هذه السياسة إيقاف أي محتوى (كائن) بالصفحة قادم من خادم آخر غير خادم مصدر الصفحة الأصلي. على سبيل المثال لا تتمتع الشفرات البرمجية الموجودة في الإعلانات الواردة على صفحة بريد إلكتروني بصلاحيات الوصول إلى باقي محتويات البريد الإلكتروني لأنها قادمة من خادم آخر غير خادم مصدر البريد الإلكتروني. ويُستخدم حقلي عنوان الإنترنت ورقم منفذ الاتصال في تحديد مصادر الكائنات حيث يُعتبر أي كائن يحتوي على قيمة مختلفة بأحد هذين الحقلين أو كلاهما كائنا مختلفا ويجب فصله. هجوم إعادة ربط اسم المجال المبين بالشكل 7 يمكن أن يخترق هذه الآلية. وفيما يلي الخطوات التي على المهاجم أن يتبعها لتنفيذ الهجوم:

1. يُقنع المهاجم المستخدم الضحية بزيارة صفحة الويب الخاصة به على سبيل المثال: (http://attacker.com).
2. يستجيب خادم تحليل اسم المجال للمهاجم بعنوان الإنترنت الخاص به ومدة صلاحية قصيرة جدًا لهذا العنوان.
3. تحتوي صفحة ويب المهاجم على شفرة برمجية تعمل على استجلاب بيانات حساسة من الخادم المراد اختراقه.
4. نظرًا لقصر مدة صلاحية عنوان صفحة ويب المهاجم فإن احتمالية إصدار متصفح الضحية استعلاما جديدا لموقع المهاجم كبيرة جدا.
5. هذه المرة يستجيب خادم تحليل اسم المجال للمهاجم بعنوان الإنترنت الخاص بالخادم المستهدف.
6. يقوم متصفح الضحية بتوصيل الشفرة البرمجية التي استلمها من المهاجم في (3) إلى الخادم المستهدف والتي بدورها تستجلب

البيانات التي يرغب المهاجم بالحصول عليها. لاحظ أن الخادم قد أعطى هذه البيانات لأحد مستخدمي الشبكة القانونيين.

7. أخيرا يقوم متصفح الضحية بنقل البيانات التي تم التقاطها من الخادم الهدف إلى المهاجم.



شكل 7. خطوات هجوم إعادة ربط اسم المجال.

مبدئيا يمكن عرقلة هذا الهجوم باتباع تقنية تعرف بتقنية التعليق. حيث يقوم المتصفح دائمًا بتخزين عنوان الإنترنت الذي يتحصل عليه من أول استعلام خلال المدة الكاملة للجلسة ولا يقوم بأي استعلامات أخرى عن نفس المجال، مما يمنع المهاجم من استخدام الاستعلام الثاني وبالتالي إيقاف الهجوم. وعادةً ما تقوم المتصفحات بتخزين المعلومات مؤقتا حتى يتم إعادة تشغيلها. ولكن هذه الطريقة ليست مجدية في كل الحالات وذلك لأن المكونات الإضافية في المتصفح (مثل javascript) قد تستخدم استعلامات خاصة بها بدلاً من الاعتماد على ذاكرة التخزين المؤقت لنظام أسماء المجالات في المتصفح. كما أن اتباع مثل هذه التقنية يعد انتهاكا صريحا لمعايير بروتوكول نظام اسم المجال التي تنص على احترام قيم مدة الصلاحية لسجلات الموارد وذلك لموازنة الازدحام على الشبكة. لذا فأن اتباع هذه التقنية يقلل من موازنة توزيع الازدحام بالشبكة والتي يهدف مصممو بروتوكول نظام اسم المجال للمحافظة عليها قدر الممكن. بالإضافة لما سبق يناقش [28] العديد من نقاط الضعف الممكنة عند تنفيذ هذه التقنية ومنها مثلا أن المهاجم قد يجبر متصفح الضحية على إجراء الاستعلام الثاني بإخراج خادم الويب الخاص به من الخدمة.

جـ. *القنوات السرية لاختراق بروتوكول نظام اسم المجال*

القنوات السرية هي نوع معروف من أنواع الهجمات الأمنية على شبكات البيانات الرقمية وهي آلية لتحقيق النقل غير المصرح به للمعلومات. غالبا ما يتم إنشاء القنوات السرية على قنوات الاتصال الموجودة واستخدامها بطريقة غير قانونية. يمكن أن تكون القنوات السرية مثل أي قناة اتصال أخرى أحادية أو مزدوجة. وكغيرها من الهجمات الأمنية فإن فئات مختلفة من القنوات السرية لها خصائص مختلفة من حيث إمكانية اكتشافها وتوفر الحلول المضادة لها ومقدار المخاطر التي تشكلها. ويعد بروتوكول نظام اسم المجال وسيلة سهلة للحصول على قناة سرية وذلك لطبيعته الموزعة والتكرارية على الشبكة. يمكن تلخيص أسباب ملاءمة البروتوكول كقناة سرية بالنقاط التالية:

- البروتوكول لا يمكن تجنبه عمليا لتحقيق أي اتصال على الشبكة فهو على رأس البروتوكولات المدرجة بالقائمة البيضاء لكل الأجهزة الموجودة بالشبكة.
- وجود أنواع مختلفة من الاستعلامات والإجابات وكذلك إمكانية تضمين الكثير من المعلومات الإضافية بها يتيح للمهاجم أساليب متعددة لتكوين قنوات السرية.
- يستخدم البروتوكول بروتوكول حزم بيانات المستخدم في تبادل البيانات ويتبع هذا الأخير سياسة تجاهل الأخطاء بدلاً من التعامل معها أو الإنذار عند حدوثها.

العديد من الأبحاث السابقة [31,30,29] قدمت طرق مختلفة لتكوين قنوات سرية داخل نظام اسم المجال تتراوح ما بين استعلامات بسيطة مباشرة إلى قنوات متطورة تتيح اتصال كامل في الاتجاهين. ويمكننا تصنيف هذه الطرق على النحو التالي:

استغلال الحقول. تتمثل إحدى القنوات السرية في استخدام أربعة بتات فقط من حقل رقم مُعرِّف الاستعلام لربط الاستعلام بالإجابة واستخدام البتات الأربعة المتبقية لتوصيل بيانات أخرى. إذا تمكن المهاجم من السيطرة على أحد خوادم اسم المجال بالشبكة فيمكن للمهاجم استخدام حقل اسم المضيف في الاستعلام لتوصيل بيانات أخرى لذلك الخادم الذي يسيطر عليه من أي جهاز آخر على الشبكة، كما يمكن للخادم استخدام الحقل الإضافي في الإجابة للتواصل مرة أخرى مع الجهاز مصدر الاستعلام.

استغلال الوصول إلى خادم تحليل اسم المجال. إذا كان هناك خادمان مستضيفان متعاونان يستخدمان نفس خادم التحليل فيمكنهما استخدام العديد من التقنيات للاتصال سرا. فمثلا يمكن استخدام ذاكرة التخزين المؤقت لخادم التحليل بأن يتفق هذان الخادمان مسبقا على قائمة محددة بأسماء وهمية لمستضيفين غير موجودين على الشبكة. يبدأ أحد الخوادم بالاستعلام عن بعض أسماء المستضيفين من تلك القائمة ثم يطلب الخادم الثاني القائمة كاملة من خادم التحليل. إذا كانت الإجابة (NXDOMAIN) مخزنة بذاكرة خادم التحليل عن اسم المستضيف x من القائمة الوهمية فهذا يعني أن الخادم الأول قد قام بالاستفسار عنه وبالتالي يعتبر الخادم الثاني أن الخادم الأول يريد توصيل القيمة الرقمية 1 وإذا لم يكن كذلك فإن القيمة هي 0.

استغلال ملحقات نظام اسم المجال. في هذا النوع يتم استغلال بنية حزمة بيانات بروتوكول نظام اسم المجال للحصول على مساحات فارغة داخل الحزمة يمكن استخدامها كقناة سرية [31]. يمكن تطوير هذه التقنية للحصول على قنوات سرية تصل سعتها إلى 512 بت.

يوجد العديد من التقنيات المقترحة لتقليل استخدام بروتوكول نظام اسم المجال كقناة سرية. كالفصل بين واجبات الخوادم، حيث يتم الاحتفاظ بخوادم التحليل العودية بشكل منفصل عن خادم الاسم الرئيسي وأيضًا يتم الاحتفاظ بخادم تحليل أسماء المستضيفين داخل الشبكة المحلية بشكل منفصل عن ذلك الذي يوفر تحليل الاسم للمستضيفين الخارجيين. علاوة على ذلك يجب أن يتم إخفاء محلل الاسم الداخلي خلف جدار للحماية. هذا الحل والعديد من الحلول الأخرى تمت مناقشتها في [32]. وتجدر الإشارة إلى أن ملحق الأمان لا يوفر أي حل لهذا النوع من الهجمات لأن جميع المعاملات التي تقوم بها الأطراف المتعاونة لإنشاء القناة مشروعة تمامًا. الأسوأ من ذلك أن ملحق الأمان يمكن استغلاله للحصول على قنوات سرية بسعات أكبر.

6. الاستنتاج

إن دفاعات تهديدات بروتوكول نظام اسم المجال كغيرها من دفاعات التهديدات الأخرى في مجال أمن المعلومات الرقمية تحتم على المدافعين أن يكونوا على علم بكل ما يستجد من تقنيات الاختراق المتاحة للمهاجمين وأن يكونوا على استعداد تام للعمل بسرعة على التخفيف من خطورة أي تهديد مكتشف حديثا. علما بأن المهاجمون المقصودون في هذه المقالة ليسوا أفراد بإمكانيات بسيطة أو مجموعات مبعثرة تقوم بأعمال تخريبية لأجل المتعة. إنما هم مجموعات منسقة جيدا وموزعة على مستوى العالم ولها معرفة كاملة ببروتوكولات الإنترنت. هذه المجموعات لا تحركها بالضرورة المكاسب المالية وإنما قد تكون لها أهداف أكبر كالأهداف السياسية أو العسكرية. ولأن بروتوكول نظام اسم المجال يعتبر الركيزة الأساسية للإنترنت ويعد أمرا حاسما لتشغيلها فيجب أخذ كل تهديد لهذا البروتوكول على محمل الجد، ويجب بذل كل جهد ممكن لتقليل خطورة أي محاولة للهجوم عليه. آخر هجوم واسع على مستوى الإنترنت استهدف البروتوكول كان هجوم إيقاف الخدمة ضد خوادم الجذر، وقد تم التعامل معه بسرعة وبأقل تأثير ممكن على مستخدمي الإنترنت [19]. ويعد التغلب على هذا الهجوم مؤشرا جيدا للحالة الراهنة لأمن البروتوكول.

بالإضافة إلى تهديد البروتوكول في حد ذاته، هناك العديد من التهديدات التي تستهدف تطبيقات محددة تعمل عليه، ويتطلب التخفيف من خطورة هذه التهديدات تصحيحا فوريا وترقية للتطبيقات الضعيفة.

من خلال مناقشتنا للتهديدات الرئيسية لبروتوكول نظام اسم المجال والدفاعات الممكنة يبدو أن ملحق الأمان يحل العديد من المشكلات المرتبطة به إلا أن هذا الملحق يعد بمثابة إعادة لتصميم البروتوكول بوضع الأمان في الاعتبار، مما يجعل تكلفة تنفيذه باهظة. فهناك التكاليف الأولية كالتوقيع الرقمي لكافة سجلات الموارد الموجودة بخوادم المجالات وتوزيع

المفاتيح بالإضافة لتكاليف التشغيل، كتوفير سعة إضافية كبيرة على الشبكة. أضف إلى ذلك أن هذا الملحق لا يمكنه العمل بكفاءة إلا إذا تم اعتماده على نطاق واسع بالشبكة. وبالنظر للعدد الهائل لخوادم البروتوكول التي تعمل على الإنترنت اليوم نتوقع أن تكون عملية الترقية مكلفة للغاية. كما يجب ألا ننسى أن ملحق الأمان قد تمت دراسته وقبوله كحل للتهديدات المعروفة حاليا. لذا وفقط بعد تطبيق هذا الملحق فعليا على نطاق واسع يمكن للمرء أن يعرف ما إذا كان سيجلب نقاط ضعف أخرى أو خلق فئة جديدة من التهديدات، فمثلا يناقش المؤلف في [33] إمكانية وتبعات أن يكتشف المهاجم مفاتيح التوقيع الخاصة بخادم اسم المجال.

كان هدف هذه المقالة هو إعطاء فكرة عامة عن آلية عمل بروتوكول اسم المجال ومن ثم تقديم مسحا موجزا عن الاختراقات الأمنية الممكنة للبروتوكول عن طريق التلاعب على آلية العمل تلك. وبهذا نأمل أن تجعل هذه المقالة المهتم بالبحث في موضوع أمن بروتوكول اسم المجال على دراية باتجاهات البحث الحالية في هذا الموضوع، وأن تمهد الطريق أمامه للتعمق أكثر في دراسة خبايا عمل البروتوكول وكذلك في دراسة طرق التحايل عليه واختراقه وهو ما يؤهله فيما بعد لاكتشاف ثغرات أمنية جديدة بالبروتوكول وذلك بتطوير أحد الطرق السابقة لاختراق البروتوكول أو باقتراح أسلوب آخر جديد. للوهلة الأولى قد يبدو أن اكتشاف أسلوب جديد لاختراق بروتوكول تمت دراسته بشكل كبير ويعمل فعليا لسنوات طويلة أمرا صعبا إن لم يكن مستحيلا، إلا أن تاريخ البحث في مجال أمن المعلومات يخبرنا عكس ذلك، فأمن المعلومات ما هو إلا سجال من الجولات المتواصلة بين قراصنة المعلومات الساعون لاختراق شبكات المعلومات والقيام بالأعمال التخريبية من جهة وبين من يحاول التصدي لهجمات هؤلاء القراصنة لتأمين شبكات المعلومات من الجهة الأخرى.

المراجع

[1] P. Mockapetris and K. J. Dunlap, "*Development of the domain name system*", in *Symposium proceedings on Communications architectures and protocols*, SIGCOMM '88, (New York, NY, USA), pp. 123133, ACM, 1988.

[2] P. Vixie, *"Extension mechanisms for dns (edns0)".* http://www.ietf.org/rfc/rfc2671.txt, August 1999.

[3] P. Mockapetris, "*Domain names - implementation and specication."* http://www.ietf.org/rfc/ rfc1035.txt, November 1987.

[4] E. Lewis, "*DNS zone transfer protocol (axfr)*." http://tools.ietf.org/rfc/rfc5936.txt, June 2010.

[5] M. "*Ohta, Incremental zone transfer in DNS*." http://tools.ietf.org/rfc/rfc1995.txt, August 1996.

[6] D. Barr, "*Common dns operational and conguration errors*." http://www.ietf.org/rfc/ rfc1912.txt, February 1996.

[7] P. Vixie, "*A mechanism for prompt notication of zone changes (dns notify)."* http://www.ietf.org/ rfc/rfc1996.txt, August 1996.

[8] P. Vixie, "*Dynamic updates in the domain name system (dns update)."* http://www.ietf.org/rfc/ rfc2136.txt, April 1997.

[9] R. Perdisci, M. Antonakakis, X. Luo, and W. Lee, WSEC "*DNS: Protecting recursive DNS resolvers from poisoning attacks*," in Dependable Systems Networks, 2009. DSN '09. IEEE/IFIP International Conference on, pp. 3 12, 29 2009-july 2 2009.

[10] P. Vixie, "*Secret key transaction authentication for dns (tsig)*." http://www.ietf.org/rfc/ rfc2845.txt, May 2000.

[11] D. Eastlake, "*Dns request and transaction signatures (sig(0)s)*." http://www.ietf.org/rfc/ rfc2931.txt, September 2000.

[12] D. Eastlake, "*Domain name system security extensions*." http://www.ietf.org/rfc/rfc2535.txt, March 1999.

[13] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "*Resource records for the dns security extensions."* http://www.ietf.org/rfc/rfc4034.txt, March 2005.

[14] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "*Protocol modications for the dns security extensions*." http://www.ietf.org/rfc/rfc4035.txt, March 2005.

[15] S. Weiler and J. Ihren, "*Minimally covering nsec records and dnssec on-line signing*." http:// www.ietf.org/rfc/rfc4470.txt, April 2006.

[16] W. Hardaker, "*Use of sha-256 in dnssec delegation signer (ds) resource records (rrs)."* http:// www.ietf.org/rfc/rfc4509.txt, May 2006.

[17] M. StJohns, "*Automated updates of dns security (dnssec) trust anchors*." http://www.ietf.org/ rfc/rfc5011.txt, September 2007.

[18] B. Laurie, G. Sisson, R. Arends, and D. "*Blacka, Dns security (dnssec) hashed authenticated denial of existence*." http://www.ietf.org/rfc/rfc5155.txt, March 2008.

[19] ICANN, "*Root server attack on 6 february 2007*." http://www.icann.org/en/news/ announcements/announcement-08mar07-en.htm, March 2007.

[20] Secure64, "*Slow adoption of dnssec puts leading e-commerce companies at risk*." http://www. prnewswire.com/news-releases/slow-adoption-of-dnssec-puts-leading-e-commerce-companies-at-risk-189857881.html, Feb 2013.

[21] Geoff Huston "*DNSSEC validation revisited*" https://blog.apnic.net/2020/03/02/dnssec-validation-revisited/, Mar 2020.

[22] S. Krishnan and F. Monrose, "*An empirical study of the performance, security and privacy implications of domain name prefetching,"* in Dependable Systems Networks (DSN), 2011 IEEE/IFIP 41st International Conference on, pp. 61 72, june 2011.

[23] S. Son and V. Shmatikov, "*The Hitchhiker's guide to dns cache poisoning,*" in Security and Privacy in Communication Networks, vol. 50 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 466483, Springer Berlin Heidelberg, 2010.

[24] http://www.slideshare.net/dakami/dmk-bo2-k8.

[25] http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html.

[26] J. Jiang, J. Liang, K. Li, J. Li, H. Duan, and J. Wu, "*Ghost Domain Names: Revoked Yet Still Resolvable,"* in Proceedings of the 19th Annual Network & Distributed System Security Symposium, Feb 2012.

[27] T. King, "*Packet sning in swithced environment*." http://www.sans.org/reading_room /whitepapers/networkdevs/, august 2002.

[28] C. Jackson, A. Barth, A. Bortz, W. Shao, and D. Boneh, "*Protecting browsers from DNS rebinding attacks*," ACM Trans. Web, vol. 3, pp. 2:12:26, Jan 2009.

[29] C. Dietrich, C. Rossow, F. Freiling, H. Bos, M. van Steen, and N. Pohlmann, *"On botnets that use dns for command and control,"* in Computer Network Defense (EC2ND), 2011 Seventh European Conference on, pp. 916, 2011.

[30] L. Nussbaum, P. Neyron, and O. Richard, "*On robust covert channels inside dns,*" in Emerging Challenges for Security, Privacy and Trust, vol. 297 of IFIP Advances in Information and Communication Technology, pp. 5162, Springer Berlin Heidelberg, 2009.

[31] K. Born, Psudp: "*A passive approach to network-wide covert communication*," Black Hat USA, 2010.

[32] K. Born and D. Gustafson, "*Detecting dns tunnels using character frequency analysis*," arXiv preprint arXiv:1004.4358, 2010.

[33] "*A dnssec draft about compromised key*." http://www.ietf.org/mail-archive/web/dnsext/ current/msg12809.html, Nov 2012.