Dynamic DNS and Location Tracking – Risks and Benefits

Robert Jones

Craic Computing Technical Report 2006-1

Abstract

Dynamic DNS allows a static hostname to be associated with residential or mobile computers that are assigned dynamic IP addresses by their Internet service providers. The service is particularly useful for business travelers who use Virtual Private Networking technologies.

But this convenience comes at a price. By monitoring the fully qualified domain name (FQDN) used by a dynamic DNS client, it is possible to track the Internet location of that computer as it moves from one place to another. In some cases the Internet address can be mapped to a geographic location.

While there are legitimate uses for dynamic DNS monitoring, for most users of the technology it represents a serious risk to their privacy and one is largely unrecognized. This paper shows how simple it is to monitor dynamic DNS clients and provides examples of the information that this can reveal. It shows how monitoring might be used and abused, and it describes ways in which the potential privacy risk can be minimized.

Background

Most Internet protocols, such as HTTP or SMTP, require that client computers know the static address of the server they wish to communicate with. An address may take the form of a numeric IP address, such as 192.168.1.1, or a fully qualified domain name (FQDN), such as www.craic.com. Translation between these two forms is handled by the Domain Name Service (DNS).

However, most residential and small business computers do not have static addresses. They are assigned dynamic IP addresses by their Internet Service Providers (ISP) and these can change every time a computer is rebooted or reconnects to the network. This allows ISPs to manage finite pools of addresses efficiently. But the problem with the approach is that it becomes impossible to run a resource like a web server on one of these machines. Any client wishing to connect would need to know the IP address that was currently being used, which would appear to be impractical.

The solution is to create a static FQDN for the computer and to have that machine update a remote public DNS server whenever its IP address changes. This is referred to as "Dynamic DNS" and a number of companies offer Dynamic DNS services at low or no cost to the community.

The system consists of two components. The first is a publicly accessible DNS server that manages a unique FQDN that is owned by the client. The second is a piece of software that runs on the client computer and that updates the DNS server whenever its IP address changes. Users can then be directed to services using the FQDN as the address of the computer. The DNS server

translates that to the current IP address and a successful connection can be made. The approach is easy to set up on a client computer and updating of the DNS server requires no action on the part of the user.

The uses of dynamic DNS have now expanded considerably beyond running web servers on home computers. Users of network-enabled computer games use it to identify specific machines of other gamers. It can identify residential or mobile computers to remote mail servers as part of measures to prevent spam.

Of particular importance here is the growing use of dynamic DNS in Virtual Private Network (VPN) hardware used to connect mobile computers to corporate networks. In this application a remote user with a laptop initiates a VPN tunnel with a gateway to the corporate network. The authentication phase of this can involve several steps, most important of which is the transfer of a pre-shared secret key. As part of this phase, the gateway can optionally authenticate the IP address of the remote computer. Systems that implement this typically can be configured to allow tunnels from either any address on the Internet or from specific static IP addresses. As most mobile users are assigned dynamic addresses, this constraint is not very useful. In response to this, a number of VPN gateways now allow a FQDN for a remote computer to be included among these constraints. The remote laptop defines a FQDN at a dynamic DNS service provider, updating the corresponding IP address as it changes. The VPN gateway includes that FQDN in its list of allowable clients. The feature has been incorporated into a variety of VPN hardware, such as the NetGear FVS series and the Linksys RV series of VPN firewall routers.

The Problem with Dynamic DNS

Consider a business traveler who has a laptop configured to automatically update a remote DNS server with its current IP address. If the FQDN that was being updated by the laptop is known, or can be guessed, then anyone with modest computer skills can issue DNS queries on that name at regular intervals and monitor the current IP address.

As the traveler moves from one location to another, the IP address will change and the public DNS record for the FQDN will reflect this. The person monitoring the domain name will be able to observe the precise network locations used whenever the laptop connects to the Internet, as well as an approximate timestamp for when each event took place. Depending on the resources available to the monitor, most notably whether or not they work for law enforcement, they may be able to map that network location to a geographic location, possibly with a high degree of resolution.

The public DNS system is distributed across thousands of servers on the Internet and is used in a wide range of Internet protocols. Dynamic DNS monitoring uses nothing more than basic DNS queries and as such it offers effectively complete anonymity to the person doing the surveillance. Not only that, the target this is unable to detect that they are being observed in this manner. This represents a new form of surveillance that might be used by law enforcement for legitimate purposes or for unethical reasons by co-workers, competitors, or even stalkers, of the target.

Dynamic DNS is used by a large number of users for various reasons. For many of these, with static residential or business computers, monitoring poses no real privacy risk. But for those who travel with their laptop it could pose a serious risk to their personal privacy and business confidentiality. This risk has not been widely recognized thus far.

A DNS Monitoring Tool

The ease with which DNS records can be monitored is illustrated by this simple Perl script. It was written for a UNIX system and uses the DNS query program 'dig' that is available on most systems. It could be easily adapted for other operating systems. The script runs a DNS query on the FQDN using dig and then tries a reverse lookup with the IP address from the first query. If the IP address has changed since the last query, the script will output a timestamp, the new address and the reverse FQDN if there is one. The script sleeps for a specified interval and then repeats the DNS queries in an infinite loop.

```
#!/usr/bin/perl -w
$| = 1;

die "Usage: $0 <interval in minutes> <FQDN>\n" unless @ARGV == 2;
my $interval = 60 * $ARGV[0];
my $fqdn = $ARGV[1];

my $lastip = '';
while(1) {
    my $timestamp = scalar localtime;
    my $ip = `dig +short $fqdn`;
    chomp $ip;
    if($ip eq '') {
        print qq[$fqdn not found\n];
        exit;
    } else {
        my $hostname = `dig +short -x $ip`;
        chomp $hostname;
        if($ip ne $lastip) {
           print qq[$timestamp  $ip  $hostname\n];
        }
        $lastip = $ip;
    }
    sleep $interval;
}
```

A Simple Example of DNS Monitoring

This following example shows the results of monitoring the FQDN `craic.dyndns.org` over a period of weeks using the script that I described above. This name was set up by the author and is updated from dynamic DNS client software that runs on my laptop. The domain dyndns.org is managed by the company Dynamic Network Services, which is one of the more popular companies that offer dynamic DNS services.

```
Fri Dec  2 14:05:25 2005   208.12.16.2    nexus.craic.com.
Sat Dec  3 09:05:27 2005   64.105.42.234  h-64-105-42-234.sttnwaho.covad.net.
Mon Dec  5 08:05:34 2005   208.12.16.2    nexus.craic.com.
Mon Dec  5 15:05:35 2005   66.224.232.194 66-224-232-194.atgi.net.
Tue Dec  6 08:05:36 2005   208.12.16.2    nexus.craic.com.
Tue Dec  6 12:05:37 2005   66.224.232.194 66-224-232-194.atgi.net.
Wed Dec  7 08:05:39 2005   208.12.16.2    nexus.craic.com.
Wed Dec  7 11:05:43 2005   66.224.232.194 66-224-232-194.atgi.net.
```

```
Thu Dec  8 08:05:44 2005   208.12.16.2    nexus.craic.com.
Thu Dec  8 10:05:48 2005   66.224.232.194 66-224-232-194.atgi.net.
Fri Dec  9 15:35:50 2005   208.12.16.2    nexus.craic.com.
Sun Dec 11 09:05:56 2005   64.105.42.234  h-64-105-42-234.sttnwaho.covad.net.
```

The script was setup to monitor the FQDN at 30-minute intervals. Each line of output indicates that my laptop connected to the Internet via an IP address that was different from the last one on record. That event occurred within 30 minutes of the timestamp reported on that line.

These specific records illustrate the somewhat mundane travels of this author between my home, my office and the site of one of my clients. All three addresses had reverse DNS records, but a majority of IP addresses do not. The address 208.12.16.2 maps to the FQDN nexus.craic.com. The domain name for my company is craic.com and so this indicates that the laptop was located in my office in Seattle at those points in time. The address 64.105.42.234 maps to a FQDN in the domain covad.net. Covad is a company that manages residential and business DSL connections and so this might suggest a residential location. The subdomain *sttnwaho*, while cryptic, might suggest a location in Seattle, Washington. In reality this address represents my Internet connection at home. The third address, 66.224.232.194, maps to the domain atgi.net. This is owned by Eschelon Telecom, which provides business communication services primarily in the Western US. In reality this address represents the Internet connection of a company that I do business with in the Seattle area.

By itself, the information returned by monitoring reveals little about my specific location at any point in time. But by combining it with a modest amount of contextual information, a far more detailed picture emerges. One can see that in the week of December 5th, I went into my office each morning around 8 a.m. and then left to work at my client's location, usually mid morning, on Monday through Thursday. I did not reconnect back in the office on any of those days.

This represents a significant breach of my privacy. Simply by monitoring a specific FQDN, anyone has the potential to track my location without my knowledge and with complete anonymity. While these specific details may appear trivial, similar information could be of great interest to law enforcement staff tracking the movements of a suspected criminal or to someone trying to uncover insider information about a business deal.

Internet to Geographic Mappings

IP addresses represent precise coordinates in 'Internet space'. Given an address it is usually possible to identify the ISP that manages the block of address that it resides within. With the help of that ISP it should be possible to define the specific customer who used that address at the specified time, even if it was dynamically assigned using DHCP. In this way, the ISPs serve as the best way to map between Internet space and the geographic world that we live in. But this sort of access to ISP records is only available to government agencies such as the FBI, and even then a warrant or subpoena may be required to access the data.

There is the potential for anyone to map directly from an IP address to a geographic location, at least in certain instances. A number of geolocation companies exist that provide this sort of service, but the accuracy and resolution of the results they produce can highly variable. In particular these services will only ever work for static IP addresses. But there are also several empirical approaches that may suggest approximate geographic locations for certain IP addresses. The FQDN returned by a reverse DNS lookup may define a specific location. For example,

nexus.craic.com identifies my company and running a WHOIS query on that domain returns the street address of my office.

Although most FQDNs lack this specificity, their names may contain clues that suggest a regional location. Several of the larger ISPs embed state or city names within FQDNs and, although these can be cryptic, they can often denote regional location. For example, Comcast, which offers Internet access throughout the US, includes a two-letter abbreviation for the State in which its subnetworks are located. So one can infer that the name c-24-147-193-140.hsd1.ma.comcast.net is located in Massachusetts based on the 'ma' subdomain. Similarly the subdomain roch.mn.charter.com locates a subnetwork in the vicinity of Rochester, Minnesota.

The IP address can be used as a WHOIS query to identify the owner of the network block that contains it. This may only identify the ISP that operates that subnetwork but that, in itself, can be useful, For example, a query on 208.12.16.2 shows that assigned to Seanet Corporation and further investigation shows this to be a regional ISP based in Seattle.

In some cases using the IP address or FQDN as a URL in a web browser will reveal additional information. For example, a WHOIS query on the address 209.177.222.158 reveals an ISP based in Greenville, South Carolina, but using that as a URL returns the web page for Ethostream, a company that provides wireless networks for hotels. The combination of the two suggests that this target might be located in a hotel in South Carolina.

It must be noted that such inferences can be misleading. Many ISPs are able to assign addresses from several subnetworks for the purpose of load balancing. Similarly cooperative agreements between providers that involve network sharing may obscure the true location of any given address. Taken in isolation, such inferences run the risk of being wildly inaccurate but if they can be linked to other types of information they can often be extremely useful. This will be illustrated in the examples that follow.

A Broader Example

The second example of monitoring involves a colleague of the author who works as a long distance truck driver in the southern and western US. He typically accesses the Internet via wireless networks at truck stops every few days. Initially I made a guess as to the dynamic DNS FQDN that this person might be using and this was proven to be correct. Permission was obtained before undertaking any monitoring of the individual's location.

The output shows timestamps and IP addresses over the period of a month. All but three of the addresses had no reverse DNS record.

```
Mon Nov 28 08:35:31 2005   12.171.162.57
Mon Nov 28 17:35:33 2005   204.110.227.143
Tue Nov 29 15:35:40 2005   12.171.163.8
Thu Dec  1 18:05:50 2005   17.255.241.150
Fri Dec  2 08:05:51 2005   67.127.126.177
                           adsl-67-127-126-177.dsl.sktn01.pacbell.net.
Mon Dec  5 11:06:09 2005   12.171.163.9
Wed Dec  7 16:36:17 2005   12.171.163.11
Sat Dec 10 14:36:37 2005   12.184.65.4
Mon Dec 12 09:36:42 2005   206.106.237.76
Mon Dec 19 03:37:10 2005   12.171.163.10
Thu Dec 22 15:37:29 2005   12.171.163.2
```

```
Fri Dec 23 22:07:36 2005   67.127.126.177
                           adsl-67-127-126-177.dsl.sktn01.pacbell.net.
Sun Dec 25 00:07:39 2005   69.3.236.73
                           h-69-3-236-73.snfccasy.dynamic.covad.net.
```

This example is disappointing in the lack of geographic information that can be uncovered directly. The majority of the addresses fall in the 12.171.163.x block but this only identifies AT&T WorldNet Services as a network provider or ISP, which is too broad to be of any use. 204.110.227.143 is assigned to Flying J, a company that operates a large number of truck stops. 17.255.241.150 is assigned to Apple and suggests a wireless network within an Apple store somewhere. 67.127.126.177 maps to a subnetwork of pacbell.net called *sktn01*, which might suggest the city of Stockton in California, amongst other alternatives. 69.3.236.73 maps to a FQDN containing the string *snfccasy*, which suggests a location in San Francisco, California.

But even small amounts of additional information can help augment this output. It was learned from my colleague that the first few occurrences of 12.171.x.x addresses correlated with visits to Truck Stops of America locations. Therefore one can infer that other addresses in this block map to one of these locations, even though mapping to specific sites has proven impossible.

The guess that 67.127.126.177 was in the vicinity of Stockton proved to be correct, mapping to a hotel in Tracy, California, about 20 miles from Stockton. Having made that assignment with external information the first time the address was observed on December 2nd, it was then easy to locate my colleague at the same hotel on December 23rd.

This example shows how well DNS monitoring can be at tracking a target's location in Internet space, and at the same time shows how difficult it can be to map that to geographic space. But it also shows how small amounts of external information can be used to greatly improve this process.

Arbitrary DNS Monitoring

Knowing the dynamic DNS FQDN used by the target is a critical requirement for this type of monitoring. In many cases this will be unknown and it will not be possible to track a specific individual.

In order to study the effectiveness of monitoring on a larger scale, I generated a list of common surnames and used those to create FQDNs in several of the common domains used by dynamic DNS providers. I then ran DNS lookups to see which were actually defined and monitored those at arbitrary intervals, several days apart. By comparing the addresses of each FQDN over time I could infer information about their general location, type of Internet connection and assess whether or not they were moving from one site to another. None of the individuals associated with the FQDNs were known to me in advance and no identifying information other than DNS records was obtained.

Out of that arbitrary list of 160 surnames, 121 (76%) are used in FQDNs under one domain name used for dynamic DNS records with 74 (46%) used in a second domain that was studied. This suggests that many users of dynamic DNS have chosen names that can be easily linked to their real names and that might be guessed by a potential monitor. The IP addresses of many of these

targets were seen to change over time. But in most cases, reverse DNS lookups suggested that their computers were static and were simply reconnecting to the Internet at various times.

This example shows a computer making connections to the ISP Bell Sympatico in several cities in the province of Quebec in Canada.

```
Tue Nov 29 15:18:20 2005   209.226.209.33   StJerome-ppp25169.qc.sympatico.ca.
Wed Nov 30 19:48:27 2005   206.172.176.129  Quebec-ppp142424.qc.sympatico.ca.
Thu Dec  1 14:18:27 2005   64.228.22.141    St-Jerome-ppp85032.qc.sympatico.ca.
Fri Dec  2 10:48:29 2005   209.226.144.93   StJerome-ppp18879.qc.sympatico.ca.
Fri Dec  2 16:18:30 2005   206.172.176.26   Quebec-ppp142321.qc.sympatico.ca.
Fri Dec  2 16:48:31 2005   64.228.22.147    St-Jerome-ppp85038.qc.sympatico.ca.
Fri Dec  2 19:48:31 2005   209.226.144.178  StJerome-ppp18964.qc.sympatico.ca.
Sat Dec  3 08:48:32 2005   64.228.22.81     St-Jerome-ppp84972.qc.sympatico.ca.
Sat Dec  3 14:18:33 2005   216.209.235.127  HSE-Windsor-146026.sympatico.ca.
Sat Dec  3 15:48:34 2005   209.226.144.127  StJerome-ppp18913.qc.sympatico.ca.
```

If the reverse DNS records are taken at face value, the owner of this computer spends a lot of time near the cities of St-Jerome, Quebec, and Windsor. These are all relatively close to each other, with about 80 miles between St-Jerome and Quebec. Addresses in the St-Jerome block dominate the complete set of data that was collected. One conclusion is that the target is based near this city and travels daily throughout the region, connecting to the Internet at regular intervals. However some of the time intervals between connections appear short given the potential physical distances and this example may represent a stationary individual connecting to one of a pool of addresses assigned by the ISP. Without additional insight, either hypothesis could be valid.

Potential Uses and Abuses of Dynamic DNS Monitoring

Several applications of dynamic DNS monitoring present themselves. It could prove to be extremely useful to law enforcement and intelligence agencies that wish to track the movements of individuals with laptop computers. These might be people involved in child pornography, terrorism or criminal gangs for whom dynamic DNS would allow communication between machines with no fixed location. As long as the FQDN of the target computer was known, the network location could be tracked directly without having to involve phone companies or Internet service providers. It could occur in complete secrecy with targets being completely unaware that they were under surveillance.

Companies could use it to track the location of employees that were traveling or working in the field. It might allow them to check that an employee had reached a particular destination without that person having to actively check in with the company. This would presumably occur with the explicit knowledge of the target but one can conceive of companies using the technique to check that offsite employees were actually where they were expected to be at any given time.

One interesting application of DNS monitoring is to help locate stolen computers. This has been used successfully by the staff at Dynamic Network Services (dyndns.org) on several occasions already.

Monitoring might also be used for various unethical, possibly illegal, uses. A stalker might use the technique to track the movements of their target. A business person might use it to track the location of their competitors and draw inferences about their sales calls. Tracking the movements

of executives could yield valuable insider information regarding possible business deals or mergers within a company.

Legal Issues

DNS monitoring raises several interesting legal issues in relation to conventional means of surveillance such as wire taps.

DNS records can be viewed as public information as almost all Internet transactions, like web browsing, query DNS servers without asking for permission. Looking up such a record can be viewed as equivalent to looking up a person's address and phone number in a telephone directory. Therefore law enforcement personnel, or anyone else, should be within their rights to monitor these records at will, unlike a wire tap where a court order of some form is required in most countries.

In order to use Dynamic DNS the owner of a computer must have knowingly installed software that updates its IP address to a remote DNS server. By doing so, the user would seem to have implicitly agreed to make their Internet location known to the rest of the network, whether or not they understand the implications of this step. Having made, in effect, a public announcement of their current IP address, it would appear all but impossible to argue that the privacy of the user has been violated by someone that chooses to monitor the FQDN that is being updated.

These two factors combined with the anonymity and secrecy inherent in dynamic DNS monitoring could make it both an attractive surveillance tool and, at the same time, a serious risk to privacy.

Limiting the Effectiveness of Monitoring

As long as no alternative to dynamic DNS exists for certain purposes, users who rely on the service will be vulnerable to DNS monitoring. However there are certain simple actions that can help minimize the risk to their privacy.

Monitoring requires that the target FQDN is either known or can be guessed. Choosing a name that has no obvious link to its user, perhaps one that is a cryptic mix of letters and numbers, will make it difficult for someone to guess. However the whole purpose of using a dynamic DNS name is to give that address to people or software that need to identify the client computer. So steps must also be taken to limit the number of people that know the FQDN to only those with a legitimate need for it.

The software that runs on the client computer may allow the user to turn off automatic updating of the DNS server. Manual updating would allow a user to update the DNS server only when access to a remote VPN was needed. Connections to the Internet at other times could be made without DNS updates and these could not be monitored.

A solution that might be feasible for larger companies could be to set up DNS servers that had very strict restrictions on the clients that could query them. These 'private' DNS servers would exist on the public Internet but would reject DNS queries that came from computers outside the organization that managed them. Such servers would support dynamic DNS updating from client

computers and could be queried by specific corporate VPN hardware and software. However, the effort required to setup and maintain such servers could be substantial. It is possible that companies that today provide dynamic DNS services could offer secure or at least improved services that address this vulnerability.

Because DNS is such a fundamental component of the Internet, and because dynamic DNS is fairly simple extension of that, it is difficult to see how monitoring itself can be prevented. The effective approach has to be to limit the use of dynamic DNS updating to only those situations that need it and then to limit the exposure of information as far as possible.

Conclusions

Dynamic DNS monitoring poses a risk to the privacy of a limited subset of Internet users, specifically those who travel between multiple locations and who automatically update their current IP address on remote DNS servers.

A critical requirement of monitoring is the advance knowledge of the FQDN that is being updated by the mobile client. This information may be very difficult to obtain. But if that requirement has been met, then the actual monitoring of a specific FQDN is trivial and will reveal detained information about the network location of the target computer. Mapping that Internet location to a geographic location is very difficult without access to subscriber records at service providers. But in some cases geographic information can be inferred from public records and other sources.

Because the target computer tacitly updates a remote, public DNS server there can be no presumption that this information is private. Because the person performing the surveillance only queries public DNS servers, the target is completely unaware of the activity. The high volume of DNS queries from Internet activity in general effectively hides any surveillance from detection within DNS servers, preserving the anonymity of those involved.

The use of FQDNs as an authentication step in the creation of VPN tunnels offers limited additional security relative to the other steps in that process. If this optional constraint is abandoned then many laptop users would no longer need to used dynamic DNS at all.

While dynamic DNS is used by tens of thousands of people, the risk to the privacy of its users has not been widely reported. In the short term, users should be educated about this vulnerability and shown how to minimize the amount of information they unwittingly disclose. In the long term, the technology should be amended or replaced so as to preserve its benefits while removing its attendant risk.

Acknowledgements

Jeremy Hitchcock and Tom Daly of Dynamic Network Services Inc (dyndns.org) provided valuable comments on a draft of this paper and their input is greatly appreciated.

For more information please contact Robert Jones (jones@craic.com)