Beginner's Guide on Domain Name Security

Contents

Introduction

Understand the importance of your name

To reach another person on the Internet you have to type an address into your computer - a name or a number. That address has to be unique so computers know where to find each other. ICANN coordinates these unique identifiers across the world. Without that coordination we wouldn't have one global Internet.

ICANN was formed in 1998. It is a not-for-profit entity that forms a partnership of people from all over the world dedicated to keeping the Internet secure, stable, resilient to failure, and interoperable. It promotes competition and develops policy for the Internet's unique identifier systems (Internet addresses and protocol parameters and domain names).

ICANN doesn't control content on the Internet. It cannot stop spam and it doesn't deal with access to the Internet. But through its coordination role of the Internet's naming system, it does have an important impact on the expansion and evolution of the Internet.

Through ICANN's joint efforts with the Internet community we have created an environment in which it is easy to buy domain names along with the services and systems needed to support them. This in turn has encouraged competition and creativity in the industry. However, such success and movement of business to the Internet creates a need to ensure our domain names assets are properly secured.

Domain names are easy to register and relatively inexpensive to obtain. These commodity attributes often diminish the importance of domain names and consequently, the processes surrounding domain name registration, maintenance, and protection are often overlooked. This may not have had much of an impact in the early days of the Internet when recovery was managed through a small community of operators. However, in today's vast Internet ecosystem and increasingly connected world, domain names have become a critical part of individual, organizational, or corporate online identity, and therefore must be protected.

These issues can affect anyone on the Internet. To illustrate, here are two examples.

At a family reunion you all decide it might be fun to have a web site reflecting the family name to share stories and photos. So you click on the first domain name registration service provider ("Registrar") you find and register the domain name while at the reunion. After everyone returns home, the domain name idea is forgotten about. A few years elapse, then someone proposes another reunion and suggests it might be good to put a web site behind the "family" domain name. You search for the login credentials provided by the Registrar when you registered the domain name. In searching your emails and slips of paper for this information you find emails from the Registrar in your spam folder indicating that your domain name is about to expire. Unfortunately, these were received sometime in the past. You contact the Registrar[1] and find that someone else has taken the domain name and recovery may be a long and laborious process[2]. You contact the new owner of the domain name only to find they have

[1] or use tools like WHOIS or domain name search sites

[2] Uniform Domain-Name Dispute-Resolution Policy https://www.icann.org/resources/pages/udrp-2012-02-25-en
WIPO Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP)
http://www.wipo.int/amc/en/domains/guide/

the same family name and do not want to give it up. Now you must return to the reunion and apologize for losing the "family" name. At the reunion, one of your technically savvy relatives tells you what you should have done to have avoided losing the domain name[3].

In the second example, during an evening out with new friends, geeky Bob decides it might be a fun to throw together a web site where he can share his random thoughts with his friends. They pick the first instant web site provider they find, click on their link, come up with a domain name, and now have a site. After a few days Bob starts receiving emails from his simple web site provider warning him that he is exceeding the capacity of his account because his friends have shared the web site address with their friends and the site has become heavily visited. Bob is now popular with his friends and has stumbled on what may become a profitable service so he would like to keep the site going. In order to increase the capacity of the web site, the current provider wants an unreasonable sum so Bob looks elsewhere and finds many options with much greater performance and capacity. He has found a way to move the content of his web site from the current provider to another, however, when he studies the fine print of the agreement with the current provider he finds that the domain name and the web services are part of a single product and the domain name alone cannot be transferred to another provider without the risk of loss. He is left with no other choices but to limit the capacity of his site and thus lose visitors, pay exorbitant fees to the current provider, or get a different domain name – ensuring he has clear control of the domain name – and hopefully getting all the users start using the new name.

The systems and services supporting domain name registration that are available today are, in general, easy to use, cost effective, and reliable. However, domain name holders ("Registrants") often overlook the details surrounding domain name maintenance, protection, and how these are practiced differ greatly among domain registration service providers.

Unfortunately it has been a painful learning curve. Just ask the many high profile companies that have learned the hard way. From forfeited domain names due to forgotten (minor) registration fees to concerted social engineering and cyber-attacks[4] on the Registrars and Registries that sell us the domain names, the need to reconsider the processes securing our Internet presence is now clear.

The consequences of inadequate controls include lost revenue and reputation due to a lost or hijacked domain name where an adversary or hacker can impersonate a site by redirecting traffic to web servers owned by them or simply deny service to a site[5].

To understand how to address these problems one must consider the various roles and relationships entities have between the domain name registrant (content provider, your website, you), end user (also you), and Registrar, Registry, and root.

---

[3] SAC010 Renewal Considerations for Domain Name Registrants
https://www.icann.org/en/system/files/files/renewal-advisory-29jun06-en.pdf
SAC011 Problems caused by the non-renewal of a domain name associated with a DNS Name Server
https://www.icann.org/en/system/files/files/renewal-nameserver-07jul06-en.pdf

[4] A brief History of DNS Hijacking – Morgan Marquis-Boire, Google
https://costarica43.icann.org/meetings/sanjose2012/presentation-dns-hijackings-marquis-boire-12mar12-en.pdf
SAC007 Domain Name Hijacking Report http://archive.icann.org/en/announcements/hijacking-report-12jul05.pdf

[5] Measures to Protect Domain Registration Services Against Exploitation or Misuse
https://www.icann.org/en/system/files/files/sac-040-en.pdf

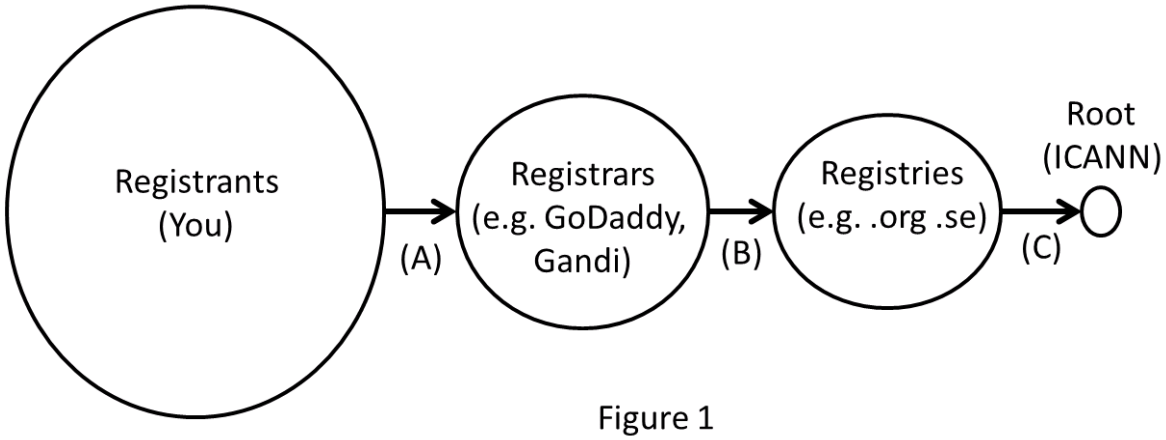

Figure 1

Referring to figure 1, (A) the Registrant typically goes to a Registrar's web site and checks the availability of a domain name – say example.org. (B) If the name is available, the Registrant pays the Registrar for the rights to use a domain name (for a minimum of one year). The Registrar obtains the domain name from the Registry (the operator running .org in the example) on behalf of the Registrant. In the process, the Registrar requests contact information for the domain name. (C) Unrelated to (A) or (B) the Registry registers and maintains their TLD (.org) at the Root which is managed by ICANN.

Each step along this chain offers opportunities to the attacker and challenges for the domain name holder.

For more background please refer to the "Beginner's Guide to Domain Names" https://www.icann.org/en/system/files/files/domain-names-beginners-guide-06dec10-en.pdf

Registration issues:

As described in the above steps there are multiple players in the registration chain. Typically a domain name is purchased from a Registrar – the retailer - (e.g., GoDaddy, Gandi) who provides registration services to the general public. The Registrar in turn registers the new domain name on behalf of the buyer (Registrant) with a Registry – the wholesaler - responsible for a particular top level domain (e.g., .org managed by Public Interest Registry or .se by the Internet Infrastructure Foundation of Sweden). Prior to this the Registries register their names (e.g., .org .se) in a single table at the "root". This allows any domain name to be looked up with only a reference to the root then successively following references to Registry (e.g., .org) then domain name (e.g., example.org) and finally web site (e.g., www.example.org).

Registrars

The strength of any chain is determined by its weakest link. Following this analogy there are a number of points along the chain that should be scrutinized from a security perspective. Refer to figure 1.

Starting with the Registrant's relationship with the DNS ecosystem (A) there are well over 1000 Registrars. With this wide range of players, choosing the right one can be a daunting task.

If the desired domain falls under a generic top level domain (gTLD) such as .com or .xyz, there is some level of security in the fact that gTLDs may only be offered through ICANN accredited registrars (see http://www.internic.net/regist.html). These Registrars must meet various requirements that help ensure your identity on the Internet is secured and stable, thus providing some comfort.

Other TLDs such as country code top level domains (ccTLD) like .se .cn .uk can be offered by registrars that do not require ICANN accreditation but must meet requirements imposed on them by each ccTLD manager. The requirements can vary depending on the maturity of a specific TLD's operations and national laws. Registrars selling domains under some ccTLDs may well have more than adequate requirements to ensure your domain name is safe and secure. But, as demonstrated recently (see http://costarica43.icann.org/meetings/sanjose2012/presentation-dns-hijackings-marquis-boire-12mar12-en.pdf), others may still be on the early part of the learning curve and therefore may require a bit more scrutiny.

Since any registration portal is potentially vulnerable to attack via data insertion or social engineering regardless of TLD type, it is incumbent on the Registrant to make an informed choice of Registrar. In an effort to assist in this, ICANN's Security Stability Advisory Committee (SSAC) developed a list of questions to ask prospective Registrars. This can be found at https://www.icann.org/en/system/files/files/sac-044-en.pdf "A Registrant's Guide to Protecting Domain Name Registration Accounts". These include:

- What approach does the Registrar use to prove the Registrant's identity to thwart impersonation, social engineering hijack attempts, lost password recovery, transfer scams? Legal documents, government issued identification, etc?
- What sort of management interface is used to ensure only users the Registrant authorizes can access account and WHOIS information, name server, DNSSEC keys, and other technical parameters? Username and password (complexity and update requirements), two-factor authentication, one-time-passwords, digital certificates, SMS, telephone callback…? Is the Registrar's web site protected with HTTPS/SSL using a valid certificate? Is there per-domain or overall account access? How is account data secured against breach?
- How does the Registrar notify the Registrant of changes to their account or technical information? Email, call… Is there access to logs for account activity / updates / reporting / auditing?
- Does the Registrar support options to block unauthorized transfer of a Registrant's domain name or modification? Can this be performed at the Registry level (e.g., Domain Lock)? Does the Registrar provide any options to avoid unintended expiry of a domain name?
- How is communication with Registrant secured? Secure email (S/MIME, PGP), postal mail, telephone, SMS?
- Does the Registrar offer services to monitor failure/change/WHOIS/impersonation/hijack attacks on the Registrant's domain name?
- Does the Registrar support DNSSEC, i.e., can they accept and register DNSSEC key material?
- If desired, will the Registrar handle DNS and DNSSEC services for the Registrant? If so, is there a brief description of how and by whom this DNS hosting service is provided? How is it secured and how will it scale in the face of natural traffic growth and attacks?

- Does the Registrar have a streamlined process for transferring domain names to and from the Registrar should the Registrant elect to do so?
- Does the Registrar offer privacy protection services?
- Does the Registrar have published documentation on incident and abuse response practices including what assistance if any may be provided to the Registrant in registration disputes.
- Does the Registrar pass and maintain any third party audited certifications such as PCI, ISO 27000, SysTrust[6]?

Although it is unlikely that Registrars can respond to all these questions with the highest assurances, they are a good starting point to assess whether the Registrar has made DNS security part of their overall business and therefore provide the Registrant with the domain name protection and peace of mind to focus on other aspects of their business. Some Registrars publish FAQs or other documents enumerating their services to make this process easier.

Registry

At the Registry level there are a wide range of TLD choices (.com, .biz, .iq…) including non-Latin (ملیسیا, 中國,台灣, سنوت) and the same concerns over secure practices must be taken into account here.

As stated earlier, ICANN contractual requirements[7] provide some safety when it comes to gTLDs and ccTLDs base their requirements on national laws and market forces.

Drawing from the SSAC guide once again, key aspects affecting DNS stability, security and resiliency include:

- Is the Registry's DNS infrastructure capable of handling the capacity and geographical diversity of the Registrant's customers? Is there sufficient redundancy and secure practices in place to protect against, recover from, and operate in the face of attacks (e.g., DDOS). A general description of the Registry's DNS infrastructure (number of name servers, geographical distribution of same) is helpful here.
- Has the Registry met any certifications such as ISO27000 and/or subject to other 3rd party audits? These are important in getting a sense of overall system security and the practices backing them up.
- How does the Registry secure communications with Registrars? EPP?
- What sort of controls does the Registry support to ensure domain names are not illegally transferred or parameters modified, e.g., do they support Domain Locks?
- Does the Registry support DNSSEC and does it accept DNSSEC records from Registrars?
- Who else has access to the Registry's zone file? This may be a concern for some who want to avoid rampant monitoring. How often is WHOIS data updated/maintained?
- Does the Registry have documented policies regarding abuse and malicious domain names and adherence to local governmental regulations? Such policies are critical to streamlining Registrant response to phishing attacks on their domain or exceptional circumstances such as Registrar failure.

---

[6] ISO: http://en.wikipedia.org/wiki/ISO/IEC_27000-series SysTrust: http://www.webtrust.org/ PCI: http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

[7] Registrar Accreditation Agreement https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en

Obtaining such detailed information directly from all TLDs may not be possible (see http://www.iana.org/domains/root/db for contact information or search for the registry's web site), however, these questions form a reasonable basis from which to determine the security, stability, and resiliency reputation of a Registry.

Root

Finally it may be valuable to understand the root's role and its relationship with the Registries (C). In some ways the root is just another Registry but acts as the single top level phone book directing queries to the other Registries. This means that every DNS lookup on the Internet at one point starts with a query to the root to determine where a Registry's DNS servers are (i.e., the server IP addresses). This is followed by a query to these servers and eventually a query to the name servers handling the Registrant's domain name.

Given its critical nature the root's infrastructure is distributed both organizationally and geographically across 12 organizations and, as of this writing, almost 400 servers. The content of the root zone file is public and the processes governing every aspect of Registry-Root communications is documented and published.

From the Registrant's perspective, there may appear to be little choice here, but the processes and policies that govern the Root are developed by the Internet community, including the Registrants and end users, in a bottom-up, multi-stakeholder process. DNSSEC at the root is a clear example of this where its deployment, design, and regular management of key material is performed in partnership with Internet community members.

Steps you can take to secure your domain name

Making sure that you register the name to the correct entity, i.e., not to a third party supplier.

With the wide variety of web hosting offerings, the chain of domain name ownership is not always well defined. A lack of clarity here may cause difficulty later in resolving disputes, responding to accusations surrounding phishing or spam, changes to your DNS or web hosting infrastructure, or corporate ownership. Therefore when contracting the services of a one stop shop, cloud services, or even a Registrar to handle your IT infrastructure, be sure your domain name is registered to you and you have clear title. Hosting companies are not always Registrars and Registrars do not always run their own hosting services.

The same questions you might ask a Registrar should apply to the hosting provider as well. For example, do they have well defined processes for transferring domain names (and web content) away from (to) their infrastructure? How do they identify you? Do they have published procedures for dispute resolution?

Registrar, Registry options for securing your domain name

As described above, a Registrar may offer options that provide additional protection to a Registrant from unauthorized changes. One such domain lock is Registrar or client lock[8]. When set via the Registrar's interface, the Registry will not make any changes to registration details without first clearing the lock.

This measure cannot protect against completely compromised Registrant credentials or insider threats, but combined with automatic notification systems for changes in a Registrant's data, they do add valuable layers of protection and make attacks easier to detect.

Ensuring that you manage your names properly (i.e., do not register and forget)

The final part of the chain that is often overlooked is the internal practices of the Registrant itself. As was learned early on with the unintended expiration of a few high profile names, the relatively low cost of a domain name belies its critical value to a company's online presence and identity and therefore the need to manage it like any other critical asset.

Not only must maintenance fees be kept current, which can often be handled with auto-renew Registrar options, but responsible staff must be designated to receive and act on email alerts sent by the Registrar as well as regularly monitor the status and performance of the asset. This includes ensuring that WHOIS data and billing information is correct and has not changed. This may fall alongside other duties such as maintaining the IT infrastructure behind the domain name, but given the consequences of its loss or defacement due to redirection, monitoring domain names must be part of regular activities.

In summary:

- Understand who controls the domain name. Who is it registered to? How do you transfer the domain name to another Registrar? How do you change name servers?
- What options are there to protect your domain name from unauthorized transfer (locks, status codes)? From expiration? What sort of notification mechanisms are used to alert the Registrant to changes? To expiry?
- Regularly check the status of domain names using various tools such as WHOIS and those provided by the Registrar as well as monitoring routine emails[9] from the Registrar. If appropriate make these checks part of existing business processes.
- Protect and back up domain name account credentials. Most registrar account portals are password protected, so create strong passwords, and safeguard them. You may also want to shop for a Registrar that offers multi-factor authentication (e.g., token). Use SSL (HTTPS) when you access your domain name registration account.

[8] The status of these locks can often be seen in WHOIS records as "clientTransferProhibited", for example. A similar mechanism offered by a few Registries is Registry or server lock.

[9] So that legitimate emails can be distinguished from phishing attempts.

Usage issues:

In the first part we covered DNS security in the registration chain. We now touch on DNS security issues surrounding usage and operations. To help illustrate the various interactions that take place in a DNS lookup, we have the following example. This assumes the resolver was just turned on and so its cache is empty, i.e., it knows nothing except for the IP addresses for the Root servers:

1. You type in www.example.org. This causes a query to your ISP's resolver for www.example.org.
2. Your ISP's resolver looks for www.example.org but doesn't find it in its cache. So it forwards the query to the only servers it knows about, i.e., the Root servers.
3. The Root servers do not know the IP address for www.example.org but do know the IP addresses for .org's servers and sends them to the resolver.
4. The resolver then resends the same query to .org's servers.
5. .org's servers do not know the IP address for www.example.org but do know the IP address for example.org's servers and sends them to the resolver.
6. The resolver then resends the same query to example.org's servers.
7. example.org's servers DO know the IP address for www.example.org and sends it to the resolver.
8. The resolver then caches the result and sends the IP address for wwww.example.com to your browser.
9. Your browser creates a connection to this IP address and requests a web page.
10. The next time someone asks for www.example.org the resolver simply looks up the answer in its cache.

Picking a good DNS hosting provider

Regardless of whether the servers answering queries for your domain names are maintained by the Registrant, Registrar, or by a third party hosting provider, it is important to ensure steps are taken to secure this infrastructure. Specifically, your provider should have processes in place to maintain updated software and configurations adhering to best practices. No software is bug free so the entities managing these servers must keep up to date on vulnerabilities and corresponding patches.

Furthermore, as the number of systems on the Internet explodes, it becomes imperative that all systems are configured to avoid being used as part of an attack on others[10]. A few measures that can make a big difference are ensuring your hosting provider's:

- name servers are not configured as DNS resolvers and/or only respond to requests from legitimate sources;
- network only allows data with IP addresses from within its network to go out onto the Internet [BCP38[11]]; and
- systems are configured to limit the rate of responses to repetitive queries from the same source.

[10] https://www.icann.org/en/system/files/files/sac-065-en.pdf
[11] http://tools.ietf.org/html/bcp38

These steps will go a long way to reducing distributed denial of service (DDOS) attacks that can knock out portions of the Internet and increase all our costs.

Using modern DNS resolvers

The DNS recursive resolver is typically operated by the ISP for its customers or enterprise for its staff. The benefits of consolidating and remembering (caching) responses to common queries are well known and are one of the reasons the Internet continues to scale as well as it does. However, with the movement of business on to the Internet so too have the criminals who search for ways to attack. Redirecting users to malicious sites using a technique called cache poisoning to get the resolver to remember and distribute false data to customers is one such attack that was widely publicized in 2008[12] and resulted in mass updates to DNS resolver software.

Unfortunately many resolvers still run old vulnerable versions. Resolver operators (ISP or enterprise) should be strongly encouraged to keep their resolver software up to date.

DNSSEC

With attacks such as cache poisoning described above and the increased reliance on the DNS to not only convert names to numbers but also in authentication mechanisms[13], an upgrade to the DNS protocol had to be developed.

The Internet Engineering Task Force (IETF) identified the problem over 15 years ago and began developing a solution – in the same bottom-up, multi-stakeholder way in which it developed the protocols for the Internet itself. The result is a protocol called DNS Security Extensions or DNSSEC. Once fully deployed DNSSEC can be used to ensure what you put in the DNS cannot be surreptitiously modified. This will not only make it more difficult for an attacker to redirect you to their web site or steal your email but also ensures all DNS data will be protected across organizational and national boundaries. DNSSEC has been deployed at over 70% of the Registries and the Root, DNS software supports it, and there are ccTLD incentives to deploy it. However, adoption of DNSSEC by Registrants has been meager[14] due to lack of awareness and, though increasing, enabling DNSSEC validation on resolvers remains low[15].

Demand for easy to use DNSSEC solutions by Registrants is needed if DNSSEC is to have a real impact on improving Internet security.

Get Involved

[12] https://www.dns-oarc.net/node/137

[13] E.g., Creating an account: when an email to validate your identity is sent, it relies on the DNS to know where to send it. The same is true when sending a password reminder. When obtaining a certificate to secure your web site, a similar transaction occurs. Without DNSSEC, all these actions can be compromised.

[14] Approximately ~2% of domain names have DNSSEC deployed on them.

[15] https://ripe68.ripe.net/presentations/164-2014-05-14-huston-dns-measurements.pdf

As alluded to in the Root description, there are many opportunities to get involved in developing the processes that govern the DNS ecosystem. This may be through organizations such as the Internet Society[16], the Internet Engineering Task Force[17] that created the original Internet protocols or through ICANN's various constituencies. These constituencies include but are not limited to ones that represent Registries, Registrars, ISPs, and individual users (At-Large). A list of ICANN constituencies can be found here[18].

Additional Information

Here are some useful links to information on specific topics related to DNS security.

DNS videos:
https://www.youtube.com/watch?v=72snZctFFtA
https://www.youtube.com/watch?v=2ZUxoi7YNgs
https://www.youtube.com/watch?v=6uEwzkfViSM – DNS Resource Records
https://www.youtube.com/watch?v=833Qnc-7-ug – DNS Zone Files

Other IT free training videos:
https://www.youtube.com/channel/UCmJcrJ_30p6s_OTbyTFfbqQ

DNSSEC:
http://www.infoworld.com/article/2608759/security/security-why-you-need-to-deploy-dnssec-now.html Why you need to deploy DNSSec now
https://www.youtube.com/results?search_query=DNSSEC

DNS attack videos:
https://www.youtube.com/watch?v=Ib2vdxEB-C8 - cache poisoning
https://www.youtube.com/watch?v=qftKfFVHVuY - Kaminsky exploit
https://www.youtube.com/watch?v=t6oYatt8x0E - DNS changer
https://www.youtube.com/watch?v=Gz2kmmsMpMI - cryptolocker
https://www.youtube.com/watch?v=qBXrncdEifo - Steve Gibson

Distributed Denial of Service:
https://www.youtube.com/results?search_query=DNS+ddos+attacks

[16] http://www.internetsociety.org/
[17] http://www.ietf.org/
[18] https://www.icann.org/resources/pages/how-2012-02-25-en