On the differences between apples and oranges (regarding the Donuts comment on NXDomain traffic and name collisions in .com and other existent top level domains):

Shallow examinations of Domain Name System (DNS) namespaces can sometimes lead to the conflation of divergent issues and concepts. Often, in these cases, more profound examinations expose core differences that escape less perceptive summaries. For example, there are fundamental differences between NXDomain query traffic below resolvable top-level domains (TLDs) and name collisions with applied-for strings. Many of these differences stem from the fundamental semantics and policies that surround a known quantity (such as a resolvable TLD), and something that is unknown (such as an applied-for string). In particular, the hierarchies extending from resolvable TLDs represent well known and measurable real estate, which can be accounted for, by System Administrators (SAs), during namespace planning. For SAs, these codified practices are critical during configuration and planning stages, as they allow testing and measurements to elucidate problems before configurations are solidified and become production deployments.

The measurable existence of TLDs and the expectations of their usage and policies serve as fair warning to SAs who are responsible for planning the provisioning of their namespaces. Conversely, configurations that have already been deployed around non-delegated TLD strings (which inherently have no well-known policies and structure) are already relying on the negative, implicitly. This shifts the onus from SAs (end users) onto the party that is responsible for mandating a structural change to the DNS delegation hierarchy. In addition to measurable prudence, in many cases (such as with .com) these namespaces also present longstanding (and well-defined) policy semantics, which define restrictions and the conduct of clients and Relying Party (RP) software. These codified practices are critical for RPs because the policies that pervade entire TLD delegation trees allow RPs to benefit from existing protection mechanisms. Common examples of this include Public Suffix Lists and certificate issuance policies specified by the Certification Authority / Browser (CA/B) Forum. As a single example, the CA/B Forum explicitly forbids issuance of certificates below resolvable TLDs for domains that are not demonstrably administered by a Certificate applicant. By contrast, anyone can obtain a certificate for (or below) an internal TLD (iTLD). At the core of these observations is the fact that the encroachment of a namespace on clients is quite different from the encroachment of clients on an existing namespace. This fundamental misalignment may have escaped the attention of some outspoken members of the ICANN community.

In a recent set of comments regarding ICANN's proposal to mitigate name collisions Donuts outlined some core objections to foreseen risks[1]. Within their response, Donuts maintained that the ability of registry operators (and possibly delegated registrants) to effectuate a Man-in-the-Middle (MitM) attack is unrealistic. While the methodological straw man proffered up by their response seemed erroneous, the discussion is perhaps obsoleted by a recent tutorial, given at the ``TLD Security Forum.'' At time code 1:27:20 of the audio/video stream:

http://youtu.be/XRvk6ySPwTc -- a security penetration tester provided an adhoc tutorial on the relative ease (and ubiquitous practice) of this technique,

``*... go to a Starbucks, ... set up a DHCP server ... inevitably you will see the ... internal namespace ... capture credentials or go out to a Certificate[sic] Authority and buy [a certificate], you do a Man-in-the-Middle ... you have their AD creds, you log into the VPN ... wham bam, we're all set!*''

Many of the remaining comments in the Donuts response outline a concern about a superficial analogy drawn between the effects queries that result in NXDomain responses for undelegated TLDs and queries that result in NXDomain responses below delegated TLDs (such as .com). The implication of this inapt analogy is that the commentator's grasp of fundamental policies and implication in the broader ecosystem that includes DNS (but is necessarily broader) is lacking, as we discussed in the opening of this redressment.

---

[1] http://forum.icann.org/lists/comments-name-collision-05aug13/msg00030.html

One potential summary of the disconnect that likely prompted the statement from Donuts is that the set of risks posed by, and the set of potential repercussions that will likely be felt from, new gTLDs is necessarily broader than just DNS queries and responses. The systemic effects that come from interactions before, during, and after DNS transactions must be accounted for. Indeed, it is for reasons such as this that assessing risk only by measuring query rates is wholly insufficient, and naive.

In layman's terms: NXDomain responses to queries at the second level in the .com TLD are (i) not comparable to expected NXDomain response at the top level; and (ii) in any event knowable and planned for by SAs.

Eric Osterweil, Ph.D.
Principal Scientist
eosterweil@verisign.com
VeriSign, Inc.