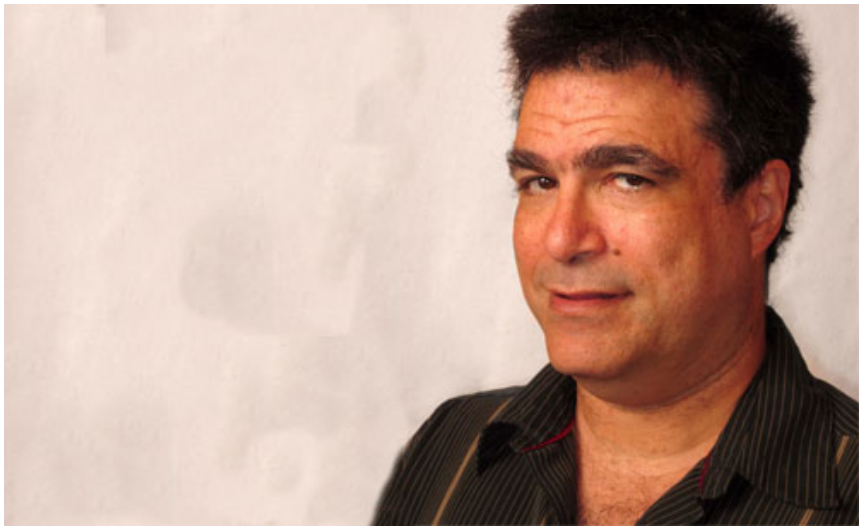
Monday, August 30, 2010

lars REICHELT “We know that we have to improve”

A disturbance in the force

This article was posted by Editor on Aug 30th, 2010 and filed under Nathaniel Borenstein, Opinion, Top. You can follow any responses to this entry using RSS 2.0. You can also leave a comment below this article



[By Nathaniel Borenstein]

The Internet is quietly being replumbed. That shouldn't surprise anyone involved with it; the Internet is always being replumbed. But you might be more surprised to learn that the next few years will bring an unusual burst of changes in that plumbing, some with great potential consequences for anyone who relies on the Net.

By its plumbing, I'm refer to the protocols and software that make the core features of the Internet work. These have been evolving steadily since 1969, but I don't think any period since the early 1980s has experienced as much change as we'll see over the next few years.

Like anything new, these changes will bring both threats and opportunities, but in this case probably more threats than opportunities. Each critical part of your infrastructure is potentially at risk from any fundamental change in the infrastructure, and we are looking at several such changes in succession.

The next big things

DNSSEC — For years experts have warned that the domain name system, one of the most important subsystems on the Internet, is at risk from malicious actors. All sorts of schemes are possible if you can hijack someone else's domain name. DNSSEC makes domain hijacking much harder and, as a result, makes it more reasonable to trust the identities of Internet sites. It is the foundation for a more trusted Internet.

After years of work, a milestone was reached this year when the root domain was signed with DNSSEC. Over the next few years, more and more sites will try to protect their identities and reputations with DNSSEC. The potential for breaking older or unusual DNS implementations can't be ignored, but any organisation that has a lot invested in its domain name should consider using DNSSEC to protect it from hijacking, and to reassure end users.

IPv6 — The Internets protocols were designed to facilitate what almost everyone thought was an absurdly big network — over 4bn computers. Less than 30 years later, we all know (as I said in 1983, mostly to dismissive laughter) that the 4bn addresses enabled by IP version 4 (IPv4) are not enough. To keep the net from fragmenting, to facilitate universal communication, and to avoid having the Internet's growth stop dead in its tracks, it is

essential that the world convert to IPv6.

Adoption of IPv6 has been slow, but there's a good reason to expect that to change: halfway through 2011, the supply of IPv4 addresses will simply run out. There are all sorts of half-measures and hacks that can postpone things a bit further, but by now it's clear that the future of the Internet requires IPv6. Despite the many person-centuries of work that have gone into IPv6, the transition is highly unlikely to be smooth and painless for everyone.

International e-mail addresses — For as long as there has been Internet e-mail, addresses have been limited to the ASCII character set. Spanish speakers can't use the letter "ñ" even if it's part of their name, and Germans similarly have to do without their "ö". They've been remarkably patient with what is, from their perspective, a gross inadequacy in e-mail standards. But the people who have it worst, of course, are the Asians, all of whose characters are forbidden in traditional e-mail addresses.

After many years of wishing, arguing and working, the Internet Engineering Task Force (IETF) is closing in on a solution. Internationalised domain names (the right-hand side of the e-mail address) have been a reality for a little while now, and the IETF has been tackling the final bit, the left-hand side. This turns out to be much harder than it sounds because of the problem of backward compatibility with the old standards and all the old mailers in the world.

The solution is going to be ugly, but functional. New encodings map ugly strings like "xn--bcher-kva.ch" onto desired internationalised forms such as "Bücher.ch". Ideally users will never see the ugly forms, which are designed to be backwards compatible, but inevitably they sometimes will. Worse still, sometimes it may be impossible for a user of older software to reply to e-mail from someone with an internationalised address.

The bottom line: we'll be going through a period during which e-mail will probably not be quite as universal, or as stable, as we're accustomed to it being. Anyone with responsibility for software that processes e-mail addresses will need to make sure that their software doesn't do horrible things when these new forms of addresses are encountered.

DKIM — The fight against spam is unlikely ever to end because the miracle of Moore's Law — the same miracle that gives us ever smaller and more powerful computing devices operates in favor of the spammers. Every time we get twice as good at detecting spam, they are able to generate twice as much spam for the same price, which means that the good guys are running on a treadmill, needing to work continuously just to avoid falling behind.

One manifestation of that hard work is the DKIM standard (for "Domain Keys Identified Mail"), which specifies a procedure by which organisations can publish cryptographic keys, and sign all their outgoing mail, thus making it somewhat easier to be sure where some messages really originate.
It's far from a cure-all, but it has the potential — particularly when paired with as-yet-undefined reputation systems — to make it easier to detect spam with forged sender information, the issue at the heart of the "phishing" problem.

DKIM has been in development for several years now, and is now progressing well through the standards process.

It should be mostly invisible to end users, but it will keep mail system administrators busy for a while. As they learn to configure their outgoing mail for signatures, and to check their incoming mail for signatures, there is a strong potential for destabilising the e-mail environment in general. The most likely symptom will be mail that just doesn't reach its intended recipient.

Reputation services — High on nearly everyone's list in the wake of technologies like DKIM are reputation services — trusted parties that can tell you if a message is signed as being from Joe.com and whether Joe.com is known for sending spam or other bad things over the Internet.

Though there are no standards for reputation services yet — and though they are undeniably needed — we can already see the risks and benefits by looking at the non-standardised reputation services in use today, notably blacklists of e-mail senders. These are incredibly useful, but there is a never-ending stream of problems with organisations that get added to such lists inappropriately and the administrative difficulties of getting them removed promptly.

Similar considerations will surely apply to the standardised reputation services of the future — no such service can be any better than the support organisation that deals with exceptions and problems. Any progress with reputation standards should be expected to be accompanied by transitional pains as the reputation service bureaus mature

and develop good or bad reputations themselves.

What can customers do?

Make no mistake: the coming improvements to the Internet's plumbing are a very good thing. But the implementation of each of them brings with it the potential for destabilising various aspects of the Internet infrastructure, despite the heroic efforts of the IETF to minimise that risk. Vendors can increase or reduce the risk through their quality of implementation. What can customers do?

Paradoxically, the answer is to do more by doing less. The biggest risks are inevitably found in the least professionally administered software and servers. The big cloud providers with the staff of crack programmers and administrators are at the least risk because they understand the risks well enough to take steps far in advance.

But that specialised application that your predecessor commissioned 10 years ago, and is now running more or less autonomously on an ancient server in your headquarters, could represent a huge risk.

Basically, the risk is highest where the least attention is being paid. So the best thing that most organisations can do in preparation for the coming instabilities is to use them as an excuse to clean house a bit: decommission old applications that aren't being maintained, outsource anything you can plausibly outsource to a bigger IT shop, and allocate a few programming resources to pay attention to the ones you can't decommission or outsource.
Of course, it can't hurt to ask your cloud provider or outsourcer what they're doing to prepare for the coming changes, but if they act surprised by any of them, it may be time to consider a new provider.

Ideally, the coming Internet disturbances should be viewed as an opportunity to streamline some of your oldest, least maintained, most idiosyncratic infrastructure. In a world where there are professionals who can run most of your applications for you, locally or in the cloud, it's probably time for your organisation to move beyond worrying about these kinds of changes.

Decommission the old stuff, outsource whatever you can, and the coming problems will largely be problems for someone else, not you. And that's about the best you can hope for as the Internet endures these growing pains.

- Nathaniel Borenstein is the chief scientist for Mimecast. Previously, he was a distinguished engineer for IBM Lotus Division

- **Subscribe to our free daily newsletter**
- **Follow us on Twitter or on Facebook**

Tell someone about this article

Leave a Reply

Name (required)

Mail (will not be published) (required)

Website

Recent Comments

- **dominic**: “CEO Ajay Pandey says Neotel’s ideal revenue mix is 10% from its retail consumer business, 30% from...
- **change agent**: It is a pity the CEO’s in SA outstay their welcome. There is a season for everything under the...
- **Max Peters**: THIS IS BULL****, I HAVE A FREE RIGHT AS AN ADULT TO INDULGE IN PORN WHENEVER I LIKE. I KNOW THAT I AM...
- **Greg**: Rather than revoke Neotel’s license, give out some more licenses, and try and resolve the problem via...
- **David H**: When last did you see a perfectly proportioned high ranking government official and/or politician?

Archives by Tag

Altech Apple Bharti Bharti Airtel BlackBerry BMI-TechKnowledge Cell C Dimension Data DStv Duncan McLeod Eassy Eskom Google iBurst Icasa interconnection rates Internet Solutions iPad Ismail Vadi Jeffrey Hedberg Lance Harris Lars Reichelt Mamodupi Mohlala Microsoft MTN Multi-Links MultiChoice MWeb Neotel Nokia On Digital Media Paris Mashile Phuthuma Nhleko Pieter Uys Reuben September SABC Seacom Sentech Siphiwe

Nyanda Super 5 Media Telkom TopTV Vodacom Zain ZA Tech Show

Recent Entries

- BlackBerry Pearl 3G: the Bold in disguise
- ZA Tech Show: Episode 126 – 'Sci-Fi'
- A disturbance in the force
- Cheap broadband to drive hardware sales
- Suspended SABC CEO fights back
- Kelly Group lifts Mdwaba suspension
- SABC board suspends CEO Mokoetle
- Bad Lieutenant: caged fury
- TalkCentral: Episode 8 – 'Reinstated'
- DA demands answers from Nyanda


Free
Lifetime* Navigation
On Your Nokia
Smartphone
Happy
Navigating
Download
here!
*For the lifetime of your phone
Nokia
N97 Mini
Nokia
5230
Nokia
E72
ovi
NOKIA