



ICANN – Cartagena DNSSEC Workshop

Preparing for and Rolling Out DNSSEC

<http://www.dnssec.comcast.net>

December 8, 2010



NATIONAL ENGINEERING & TECHNICAL OPERATIONS

The Role of an ISP in DNSSEC Validation

- ISPs act in two different DNSSEC roles, both signing and validating
 - *Signing*: authoritative infrastructure domains & customer domains
 - *Validating*: recursive resolvers operating across the ISP network
- ISPs operate the majority of resolvers that end users query
 - It is relatively rare for most residential end users to operate their own DNS, or to change their DNS settings to use a third-party DNS
 - In most cases, ISPs can automatically update DNS server IP addresses, such as via DHCP lease updates
- As such, good DNSSEC adoption by end users hinges on ISP adoption of DNSSEC
- ISPs rely on a chain of trust:
 - a signed root
 - a signed TLD
 - a signed domain

Comcast's Recently Announced DNSSEC Rollout

- Began moving customers to new DNSSEC-validating recursive resolvers on October 18, 2010
- We previously offered DNS redirect for NXDOMAIN responses (a.k.a. web error redirect)
 - The customers that opted-out are the *first* to migrate to DNSSEC
 - We've made clear that when the DNSSEC rollout is complete, we will no longer perform DNS redirect for NXDOMAIN responses
 - There is an I-D on DNS redirect, now updated to reflect this (draft-livingood-dns-redirect)
- This first group of customers finished migrating by late November 2010
 - Change occurs via DHCP lease update
- The rest of our customers will then migrate in roughly 1Q2011
- On our authoritative servers (thousands of domains)
 - We have signed all of our .ORG domains
 - We will sign all of our .NET and .COM domains soon after the TLDs sign
 - Some .NET domains will be signed this week, the rest within 90 days

DNSSEC Rollout Launch Tactics – High-Level Objectives

- Reach out to early adopters
- Explain very simply what DNSSEC is and why it is important to customers
- Be very clear about our plans
- Respond in real-time to questions and concerns
- Proactive outreach to affected customers and the tech community
- Prepare the people that interact with customers
- Make sure key constituencies, stakeholders, and the Internet community understands our plans

DNSSEC Rollout Launch Tactics

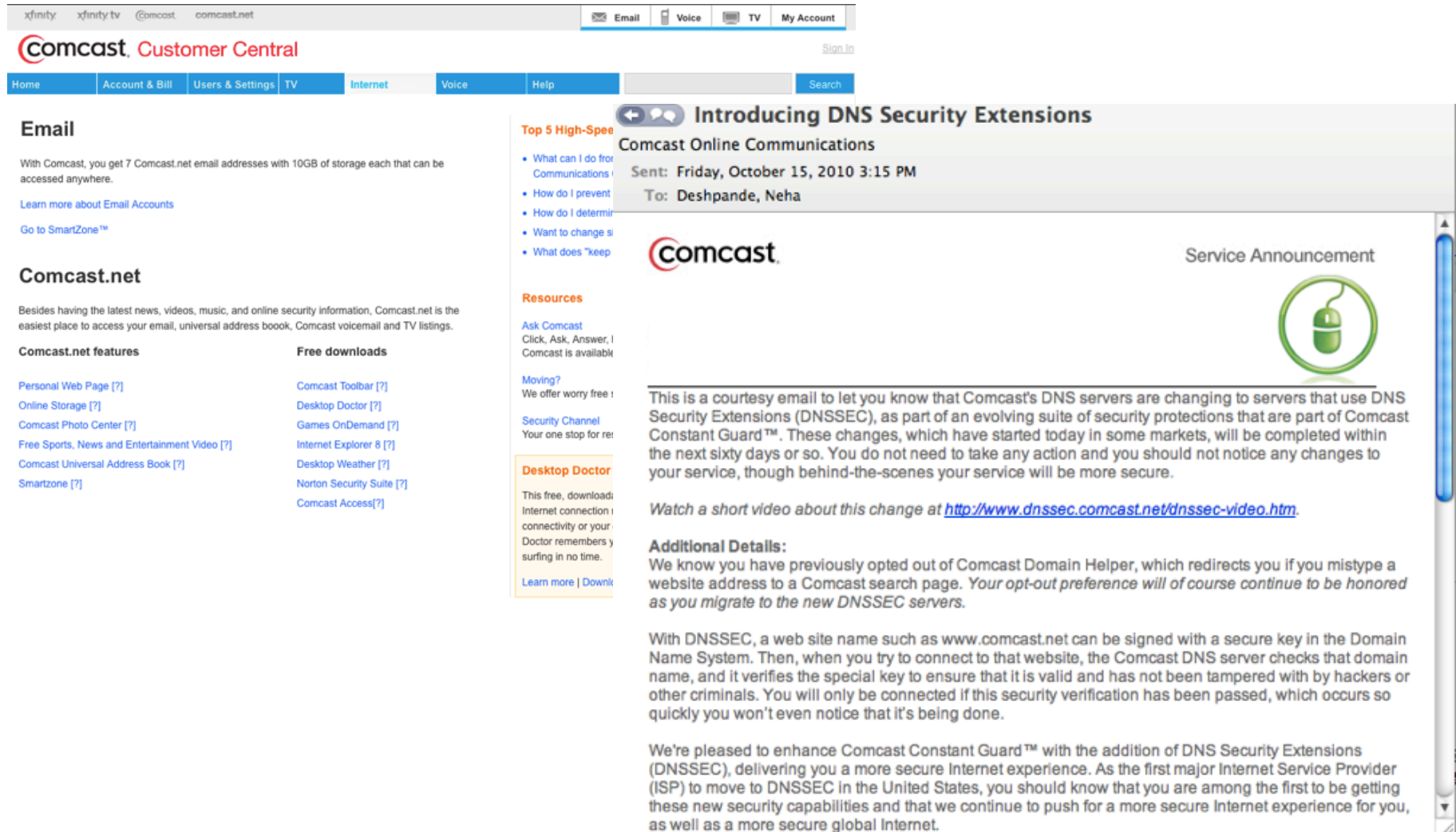
- Announced on our company blog
- This included a 2 minute overview PSA video for our customers to watch
 - Makes DNSSEC understandable for the average person
 - Explains in brief why it is important, for context
 - Presented by Kevin Pereira from G4 Network TV's "Attack of the Show"
 - Over 5,200 views – now the most popular DNSSEC video on YouTube
 - We expect thousands more views once we start migrating more customers

The screenshot shows a ComcastVoices blog post. The header includes the ComcastVoices logo and a search bar. The main content area features a blue navigation bar with links for Home, Archives, Media Gallery, About, and Help. The article title is "DNS Security Rollout Begins" by Jason Livingston. The text explains the migration to DNSSEC, its benefits for security, and the rollout schedule. A video player is embedded at the bottom of the article, showing a man in a plaid shirt speaking. To the right of the article is a sidebar with a "We'd love to hear your ideas!" section, a "Click here for Customer Support" link, and an "Authors" list.

The screenshot shows a YouTube video player. The video title is "Comcast DNS Security (DNSSEC) Public Service Announcement" by ComcastVoices. The video player shows a man in a plaid shirt speaking, with a video player overlay at the bottom that reads "DNS = Domain Name System" and "DNSSEC = Domain Name System Security". The video player includes a search bar, a "Search" button, and "Browse" and "Upload" links. The video player also shows the video title, the channel name "ComcastVoices", the number of videos "105 videos", and a "Subscribe" button. The video player includes a play button, a progress bar showing "0:16 / 2:07", and a resolution of "1080p".

DNSSEC Rollout Launch Tactics

- Email and web alerts to all customer care representatives
- Posted customer support FAQs
- Email to all customers to be migrated in the first phase



The screenshot shows the Comcast Customer Central website interface. At the top, there are navigation links for xfinity, xfinity tv, Comcast, and comcast.net. Below this is the Comcast logo and 'Customer Central' text. A navigation bar includes links for Home, Account & Bill, Users & Settings, TV, Internet, Voice, Help, and a Search box. The main content area is titled 'Email' and contains information about Comcast email accounts, including storage capacity and links to learn more or go to SmartZone. Below this is a section for 'Comcast.net' features and free downloads. On the right side, there is a sidebar with 'Top 5 High-Speed Communications' and 'Resources' sections. The central focus is an email announcement titled 'Introducing DNS Security Extensions' from Comcast Online Communications, sent on Friday, October 15, 2010, at 3:15 PM to Deshpande, Neha. The email content includes the Comcast logo, a 'Service Announcement' icon, and text explaining the rollout of DNSSEC. It states that Comcast's DNS servers are changing to use DNS Security Extensions (DNSSEC) as part of an evolving suite of security protections. The rollout is scheduled for the next sixty days or so. The email also provides a link to watch a short video about the change and additional details regarding the migration process and the benefits of DNSSEC.

Email

With Comcast, you get 7 Comcast.net email addresses with 10GB of storage each that can be accessed anywhere.

[Learn more about Email Accounts](#)

[Go to SmartZone™](#)

Comcast.net

Besides having the latest news, videos, music, and online security information, Comcast.net is the easiest place to access your email, universal address book, Comcast voicemail and TV listings.

Comcast.net features

- [Personal Web Page \[?\]](#)
- [Online Storage \[?\]](#)
- [Comcast Photo Center \[?\]](#)
- [Free Sports, News and Entertainment Video \[?\]](#)
- [Comcast Universal Address Book \[?\]](#)
- [Smartzone \[?\]](#)

Free downloads

- [Comcast Toolbar \[?\]](#)
- [Desktop Doctor \[?\]](#)
- [Games OnDemand \[?\]](#)
- [Internet Explorer 8 \[?\]](#)
- [Desktop Weather \[?\]](#)
- [Norton Security Suite \[?\]](#)
- [Comcast Access\[?\]](#)

Top 5 High-Speed Communications

- [What can I do for Communications](#)
- [How do I prevent](#)
- [How do I determine](#)
- [Want to change si](#)
- [What does "keep](#)

Resources

[Ask Comcast](#)
Click, Ask, Answer, I Comcast is available

[Moving?](#)
We offer worry free

[Security Channel](#)
Your one stop for re

Desktop Doctor

This free, download: Internet connection i connectivity or your Doctor remembers y surfing in no time.

[Learn more](#) | [Download](#)

Introducing DNS Security Extensions

Comcast Online Communications

Sent: Friday, October 15, 2010 3:15 PM

To: Deshpande, Neha

Service Announcement

This is a courtesy email to let you know that Comcast's DNS servers are changing to servers that use DNS Security Extensions (DNSSEC), as part of an evolving suite of security protections that are part of Comcast Constant Guard™. These changes, which have started today in some markets, will be completed within the next sixty days or so. You do not need to take any action and you should not notice any changes to your service, though behind-the-scenes your service will be more secure.

Watch a short video about this change at <http://www.dnssec.comcast.net/dnssec-video.htm>.

Additional Details:

We know you have previously opted out of Comcast Domain Helper, which redirects you if you mistype a website address to a Comcast search page. *Your opt-out preference will of course continue to be honored as you migrate to the new DNSSEC servers.*

With DNSSEC, a web site name such as www.comcast.net can be signed with a secure key in the Domain Name System. Then, when you try to connect to that website, the Comcast DNS server checks that domain name, and it verifies the special key to ensure that it is valid and has not been tampered with by hackers or other criminals. You will only be connected if this security verification has been passed, which occurs so quickly you won't even notice that it's being done.

We're pleased to enhance Comcast Constant Guard™ with the addition of DNS Security Extensions (DNSSEC), delivering you a more secure Internet experience. As the first major Internet Service Provider (ISP) to move to DNSSEC in the United States, you should know that you are among the first to be getting these new security capabilities and that we continue to push for a more secure Internet experience for you, as well as a more secure global Internet.


DNSSEC Rollout Launch Tactics

- Added to the Comcast ConstantGuard™ security program
- Makes this a part of a mainstream offering presented to customers regularly

comcast.net Security

Security Home | Get Protected | Get Smart | Get Help | [Outreach](#) | [Our Policies](#) | [Glossary](#) | [More Comcast](#) ▼

Constant Guard™ New Update



We are committed to providing you with the best and safest online experience possible.

As part of our ongoing efforts to continuously improve the quality of our service, we are launching Constant Guard™ for High-Speed Internet customers. Constant Guard is the result of a multi-year effort to create a comprehensive approach to protecting our customers from increasingly sophisticated online security threats.

According to Javelin Strategy and Research, there were more than 11.2 million victims of identity theft fraud in the U.S. last year at an estimated total cost of \$54 billion. Many of those thefts were made possible through the use of bots (or viruses).

The Constant Guard service consists of:

- **Customer Security Assurance:** Highly skilled security professionals who proactively contact customers to respond to issues relating to spam, and virus infected computers, as well as other security-related issues.
- **Education:** Our online security website includes real-time security alerts, tips, tools and other resources that help educate and protect consumers. For more details please visit www.comcast.net/security.
- **World-Class Technology:**
 - **Top-rated Norton Security Suite:** Provides award-winning online protection that helps guard against identity theft, viruses, hackers, spam, phishing and more. It also includes easy-to-use parental controls to help keep your kids safe online. (A \$160 value included at no additional charge.)
 - **Secure Backup & Share:** The new easier way to securely backup and share your valuable files. (2 GB storage included at no additional charge.)
 - **Desktop Applications:** The Comcast Toolbar includes anti-spyware, network-embedded anti-spam and anti-virus technologies brought to you through our partnerships with Bizanga, Cloudmark®, Goodmail CertifiedEmail™ and Return Path. In addition, we use up-to-date blocklists from Spamhaus and TrendMicro to help reduce and guard against unwanted spam.
 - **DNS Security:** At Comcast, we're pleased to enhance Comcast Constant Guard™ with the addition of DNS Security Extensions (DNSSEC), delivering you a more secure Internet experience. As the first major Internet Service Provider (ISP) to do so in the United States, you should know that you are among the first to be getting these new security capabilities and that we continue to push for a more secure Internet experience for you, as well as a more secure global Internet.

FAQs

- [What is a "Service Notice"?](#)
- [How did Comcast determine that I may have a bot?](#)
- [Did I get an infection from the page I was browsing?](#)
- [How could I have gotten a bot?](#)
- [Why am I receiving multiple "Service Notices"?](#)
- [What is a Bot?](#)
- [What is the difference between Malware and Virus?](#)

[More FAQs...](#)

DNS Security note added

DNSSEC Rollout Launch Tactics

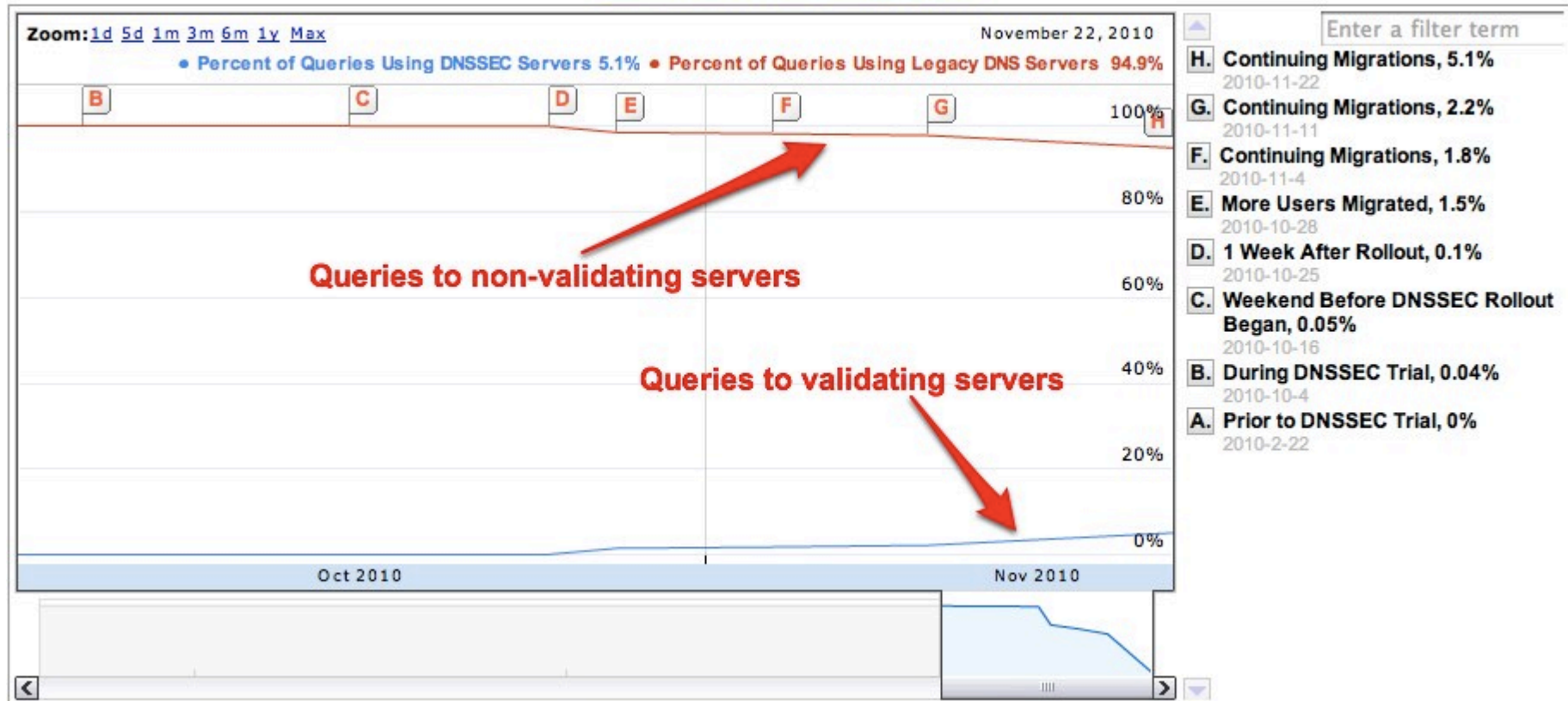
- Alerts and/or briefings to key people and relevant partners
- Online outreach
 - Broadband Reports
 - Twitter
 - Digg
 - Reddit
 - Slashdot
 - Comcast customer discussion forums
 - Various mailing lists

The screenshot shows a forum post on the website Broadband Reports.com. The page title is "[DNS] DNSSEC Rollout Begins" under the path "Forums » US Cable Support » Comcast » Comcast HSI ». The post is by user "jlivingood" (Premium, VIP, joined 2007-10-28, Philadelphia, PA, 1 kudos). The post content discusses the production rollout of DNS Security (aka DNSSEC) by Comcast, mentioning a blog post and a video from Kevin Pereira. It also provides information about DNSSEC validation failure and migration details. A second user, "beachintech" (Premium, joined 2008-01-06, The Beach, US, 5 kudos), replies with a question about users outside the Comcast network. The forum interface includes navigation links, search, and user avatars.

DNSSEC Rollout Launch Tactics

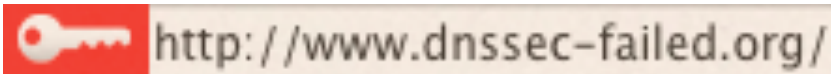
- Created a page to track our progress

Comcast DNSSEC Migration Progress



DNSSEC Rollout Launch Tactics

- Updated our DNSSEC Information Center website (<http://www.dnssec.comcast.net>)
 - Updated all FAQs, posted news update
- Launched a site to enable someone to test if DNSSEC validation works or not



THIS SITE IS ASSOCIATED WITH A DELIBERATELY BROKEN DNSSEC DOMAIN - FOR DNSSEC-RELATED TESTING PURPOSES

Using DNS Security Extensions? Then You Shouldn't See This Web Page!

----- **Deliberately Broken** -----
- **DNSSEC Validation Test Site** -

DETAILS: If your computer is using a DNS recursive resolver that has implemented DNSSEC validation, then you should NOT have arrived at this web page. As such, this web page is available for the Internet community to use for testing purposes, in order to validate whether or not DNSSEC validation is working correctly for end users. This site will be maintained permanently in support of this testing goal, so that developers and others can be assured of having a stable reference site with which to test DNSSEC validation failures, as a service to the community.

©2010 Comcast Cable | [Privacy Statement](#) | [Acceptable Use Policy](#) | [DNSSEC Video](#) | [DNSSEC Information Center](#)

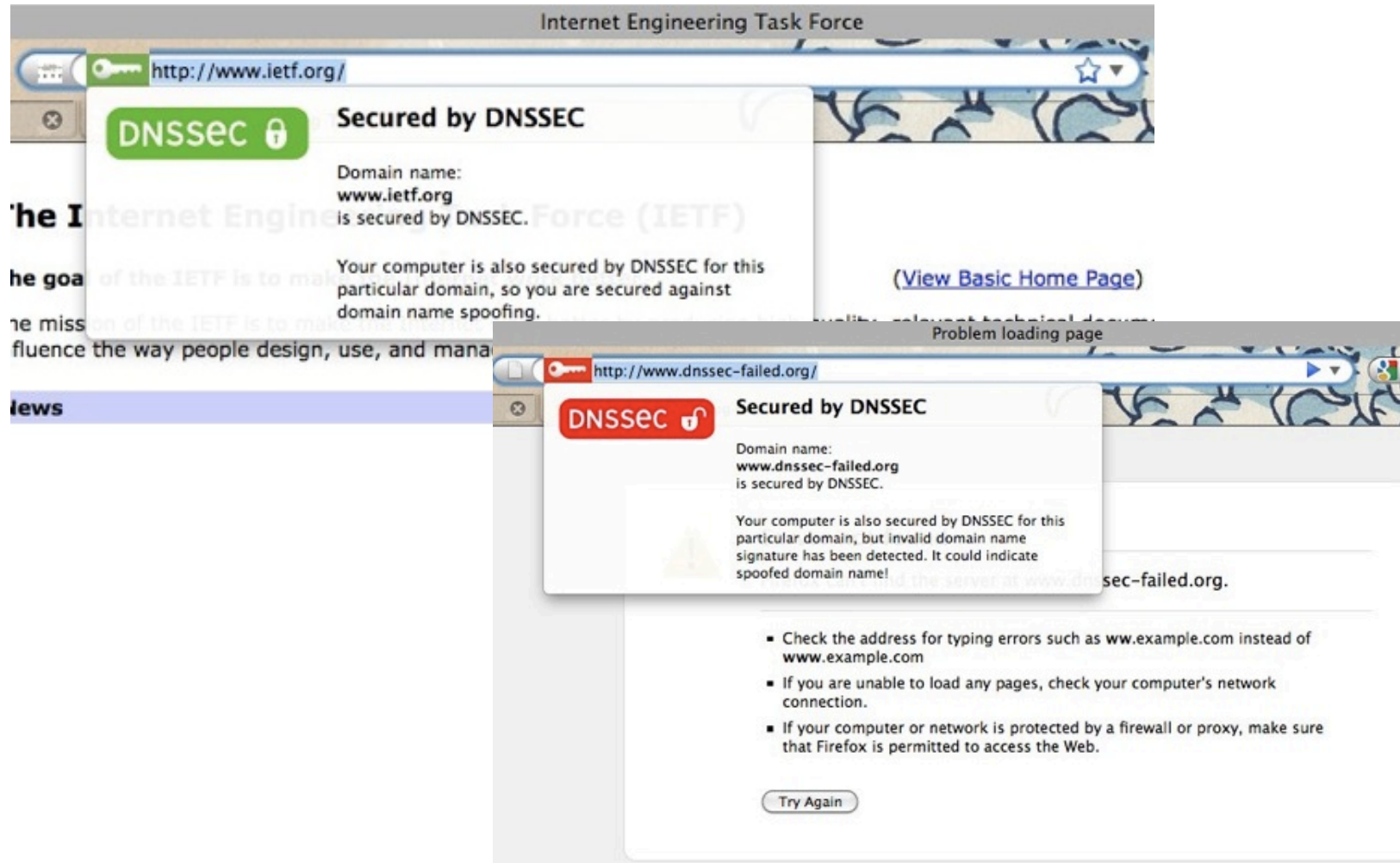


More DNSSEC Info

- [Internet Society: DNSSEC Background](#)
- [Information about DNSSEC for the Root Zone](#)
- [NTIA DNSSEC Overview and Documents](#)
- [Threats DNSSEC Can Counter](#)
- [DNSSEC Deployment Initiative](#)
- [DNSSEC Industry Coalition](#)
- [DNSSEC Tools](#)
- [DNSSEC.net](#)

DNSSEC Rollout Launch Tactics

- Recommended the Firefox DNSSEC validation add-in
- Contributed to NLnet Foundation's DNSSEC Fund to spur integration of DNSSEC validation in applications

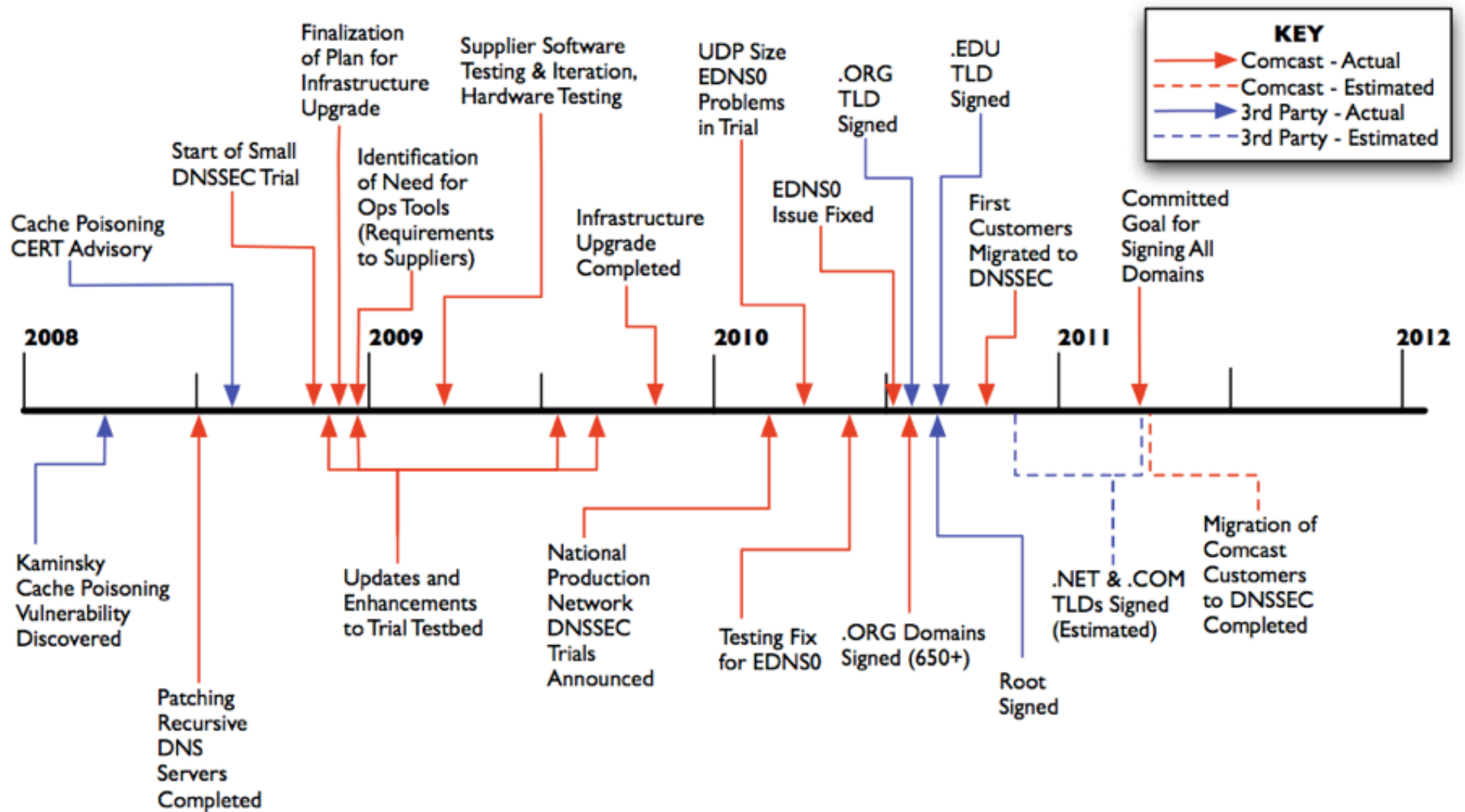


Upcoming Plans

- Start final phase of rollout in the first quarter of 2011
- Add more FAQs, especially concerning validation failures
 - Incorporate suggestions from the Internet community
- Enhance customer education materials if necessary
- Release a ~10 minute training module for each customer care representative and other personnel to complete (>24,000)
 - Preparing first line employees is critical to enabling an ISP to explain DNSSEC to customers, and troubleshoot any issues if there are problems

Prior DNSSEC Work at Comcast

- This didn't happen overnight – it took a multi-year strategic technical planning effort to prepare for, test, and launch



Prior DNSSEC Work at Comcast

- Knowing that the double whammy of DNSSEC and IPv6 was coming, we upgraded all servers and load balancers in 2009
- Comcast launched our DNSSEC trial in October 2008 to test how signing our zones and running validating resolvers would work in production
 - We initially created a test bed of 3 test DNSSEC enabled resolvers (Nominum Vantio, NLnet Labs Unbound, ISC BIND)
 - We soon found that adding keys to these resolvers was not an easy task
 - Operational tools for signing zones and rolling over keys was also lacking
- Expanded trial nationally in February 2010 to all DNS production locations
 - Added Anycast addresses (75.75.75.75 & 75.75.76.76) so our customers had an easy way to configure & test
- One objective was to identify issues early, so we had plenty of time to fix them, to remove risk from the project
 - Example was EDNS0 - did not work as expected with our load balancers
 - We and our vendor had plenty of time to develop a new GA-grade fix, QA test it adequately, soak test it, deploy it without rushing, etc.
 - Sufficient time to develop communications, training, monitoring, operational processes, etc.

Lessons Learned

- ISPs have many operational processes that may need to be adjusted to support DNSSEC validation
 - Authoritative infrastructure may need to be augmented to support signing your zones
 - Zone signing can be resource intensive
 - Chaining your zones to parents at the TLD as well as subzones can be tricky and requires planning
 - Recursive resolvers may need to be updated to software that supports validation while maintaining great scalability
- Upstream routers and firewalls may need to be addressed to support larger DNSSEC traffic for both Authoritative and Caching DNS servers
- Network Time Protocol (NTP) becomes critical for ensuring all DNS systems have the same time since encryption is being used
- Do not underestimate the training or educational materials that need to be prepared for customers and employees
- Ensure sufficient operational processes and monitoring is ready
- Make sure customers and relevant employees are briefed and understand what is changing
- THERE WILL BE VALIDATION FAILURES – FAQs and policies/procedures needed when authoritative domains encounter errors, such as RRSIG expirations

xfinity™

Thank You!

**For more information:
<http://www.dnssec.comcast.net>**



comcast®

NATIONAL ENGINEERING & TECHNICAL OPERATIONS