CENSURFRIDNS a.k.a. UNCENSOREDDNS

Thomas Steen Rasmussen
admin@censurfridns.dk

XXX RIPE 65
24-28 SEPT 2012
Amsterdam | Netherlands

Agenda

→ **Introduction**

- **DNS blocking in Denmark**

- **What is UncensoredDNS? Why was it started?**

- **Issues with DNS blocking**

- **A basic conflict: security vs. freedom**

- **Conclusion**

Introduction

- Name: Thomas Steen Rasmussen - born 1979

- Working for a Danish ISP – I manage the censored DNS servers, among other things

- Involved in IT politics since 2007ish, around when I started working my current job

- Chairman of the Danish BSD usergroup BSD-DK – see more at www.bsd-dk.dk

- FreeBSD enthusiast/fanboy since 2004

- I do consulting/development in my sparetime, email thomas@tyktech.dk for more info.

- First time at RIPE :)

Agenda

- **Introduction**
- **DNS blocking in Denmark**
- **What is UncensoredDNS? Why was it started?**
- **Issues with DNS blocking**
- **A basic conflict: security vs. freedom**
- **Conclusion**

DNS blocking in Denmark

- 2005: Pages depicting child abuse
- 2006: Copyright (allofmp3.com)
- 2008: Copyright (thepiratebay.org)
- *2009: www.censurfridns.dk launched :)*
- 2011: Unlicensed gambling sites
- 2011: Illegal pharmaceutical vendors
- 2012: Copyright (grooveshark.com)
- …. ?

DNS blocking in Denmark

- *This relates to the DK child-abuse blocking system which is automatically updated. Other blocking (like the Pirate Bay) is handled manually case by case.*

- Each ISP sends a public SSH key to the police, who adds it to the server holding the current list

- The ISP uses scp to fetch the list file regularly, like once per hour

- The list is just a list of http://domain.tld lines so it is reformatted to fit bind config syntax with standard unix tools like sed and cut.

- The list is then copied to the nameservers and loaded there.

- All domains in the list point at the same zone file (* A)

Agenda

- **Introduction**
- **DNS blocking in Denmark**
- ➜ **What is UncensoredDNS? Why was it started?**
- **Issues with DNS blocking**
- **A basic conflict: security vs. freedom**
- **Conclusion**

What is UncensoredDNS ?

- Basically, the UncensoredDNS (or "censurfridns" in Danish) service is a couple of open recursive nameservers. They run bind on FreeBSD.

- Currently two servers (although both have reduncancy, so more than two really), running on provider assigned IP addresses.

- V4 and v6 PI address space acquired recently, along with an AS number. Plans for a real anycast service using this address space are well underway.

- Need hardware and connectivity sponsors in friendly organizations/companies for the anycast project – talk to me!

Why was UncensoredDNS started?

- Friends kept asking which DNS servers to use if they wanted to visit the Pirate Bay :)

- Didn't feel like recommending OpenDNS with their nxdomain redirection.

- Google DNS didn't exist back then – and I don't really feel like recommending them either.

- Neither OpenDNS nor Google DNS had DNSSEC support or IPv6 support at the time

- Choosing a DNS provider is a matter of trust - I felt like people might have an easier time trusting an individual like me over a corporation/organisation.

- The DNS blocking system we have in place in DK is a stupid non-solution to a difficult and important problem. Using DNS servers with the blocking enabled is/was not an option.

- Clearly, a proper uncensored DNS service was needed.

Agenda

- **Introduction**
- **DNS blocking in Denmark**
- **What is UncensoredDNS? Why was it started?**
- ➔ **Issues with DNS blocking**
- **A basic conflict: security vs. freedom**
- **Conclusion**

Issues with DNS blocking

- First of all: The DNS blocking system we have in Denmark is based on some weird idea that the Internet equals HTTP and nothing else

- The STOP page gives a message explaining why stuff isn't working as expected - **if you use a webbrowser**

- But what if you were trying to send a mail to one of the blocked domains ? Only the HTTP protocol is handled. You would get a bounce four days later.

Issues with DNS blocking

- Furthermore, the Danish blocking system for child abuse pages introduces an automated single point of failure into the DNS

- This was demonstrated better than I could have asked for in March 2012, when the Danish police accidently blocked 8000 domains including google.com and facebook.com:

Posted at 01:45 PM ET, 03/02/2012

In China, Denmark, glitches in Web censorship confuse users

By *Elizabeth Flock*

Web censors got their signals crossed in China and Denmark this week.

- from http://www.washingtonpost.com/blogs/blogpost/post/in-china-denmark-glitches-in-web-censorship-confuse-users/2012/03/02/gIQATFwzmR_blog.html

Issues with DNS blocking

- DNS blocking is easy to circumvent by changing DNS server or using a proxy server. This may lead to DPI and other more intrusive blocking schemes in the future.

- DNS blocking conceals the problem without actually removing the content from the internet.

- DNS blocking is Incompatible with DNSSEC – a dishonest recursive DNS server looks just like a hacker spoofing DNS to a DNSSEC validating client.

- When a domain name is blocked in the DNS, it means that all content on that domain is blocked, including non-HTTP content - even if only some of the content is illegal.

Issues with DNS blocking

- When the local ISP DNS service is no longer considered reliable and open, Internet users may use more or less dodgy proxy services or VPN tunnels to avoid the blocking.

- This in turn may lead to CDNs seeing decreased performance, because CDNs commonly use the recursive DNS servers location to distribute load geographically.

- More DNS blocking can also mean that more alternative domain namespaces will be established, further fragmenting the Internet.

Issues with DNS blocking

- DNS blocking can serve as an "early warning system" for the very criminals it is trying to fight.

- When blocking pages that depict child abuse (like we do in Denmark), it is trivial for the operator of such pages to detect when his domain has been added to the filter.

- He now knows the authorities are onto him, he can change the domain name and keep the site going.

Agenda

- **Introduction**
- **DNS blocking in Denmark**
- **What is UncensoredDNS? Why was it started?**
- **Issues with DNS blocking**
- ➔ **A basic conflict: security vs. freedom**
- **Conclusion**

A basic conflict: security vs. freedom

- On some level, there is a basic conflict between security on the internet, and online freedom

- My nameservers can certainly be used to resolve domains with illegal content

- They may also be used in a DDOS (again) some day

- The same could be said for things like TOR and Bitcoin. They can be (ab)used for illegal purposes – but at the same time they enhance our freedom online.

- We need to be very aware of this conflict!

Agenda

- **Introduction**
- **DNS blocking in Denmark**
- **What is UncensoredDNS? Why was it started?**
- **Issues with DNS blocking**
- **A basic conflict: security vs. freedom**
- **Conclusion**

Conclusion

- The future is hard to predict :). We might see stronger / more intrusive types of blocking in the future, or we might get rid of blocking schemes entirely. Likely somewhere inbetween.

- Either way, my DNS servers will keep running as long as they are needed.

- The anycasted DNS service is ready soon-ish, this means much better redundancy.

- Anycast will also enable me to put servers in Asia, America etc. to lower latency.

The end

- This is the end of the presentation.

- If you have any questions then ask away. Find me here at RIPE65 or email me at admin@censurfridns.dk

- Join the IRC channel #censurfridns on Freenode

- Follow the twitter feed @censurfridns

- Read the blog at https://blog.censurfridns.dk (self-signed certificate - the broken CA system is not getting any of my money, but that's for another talk).

- Spread the word! Use the servers!

- Buy a t-shirt or a coffee mug, the webshop is at http://censurfridns.spreadshirt.dk (I do not make any money from the sales).

Sources / recommended reading

- *Internet Society Perspectives on Domain Name System (DNS) Filtering @* http://www.internetsociety.org/sites/default/files/pdf/dns-filtering_20110915.pdf

- *Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill @* http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf

Questions ?

?