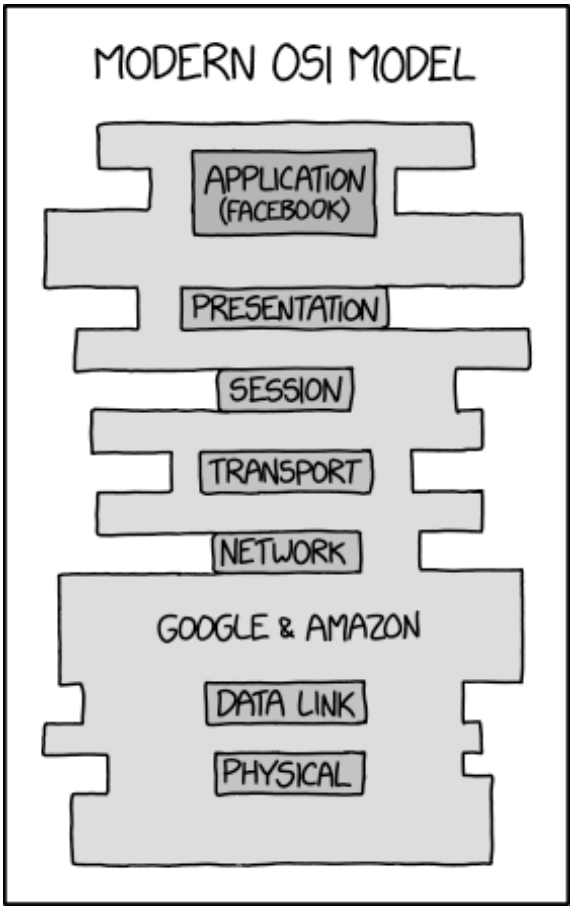


Computer networking in the real world

Mehul Motani
NUS/ECE

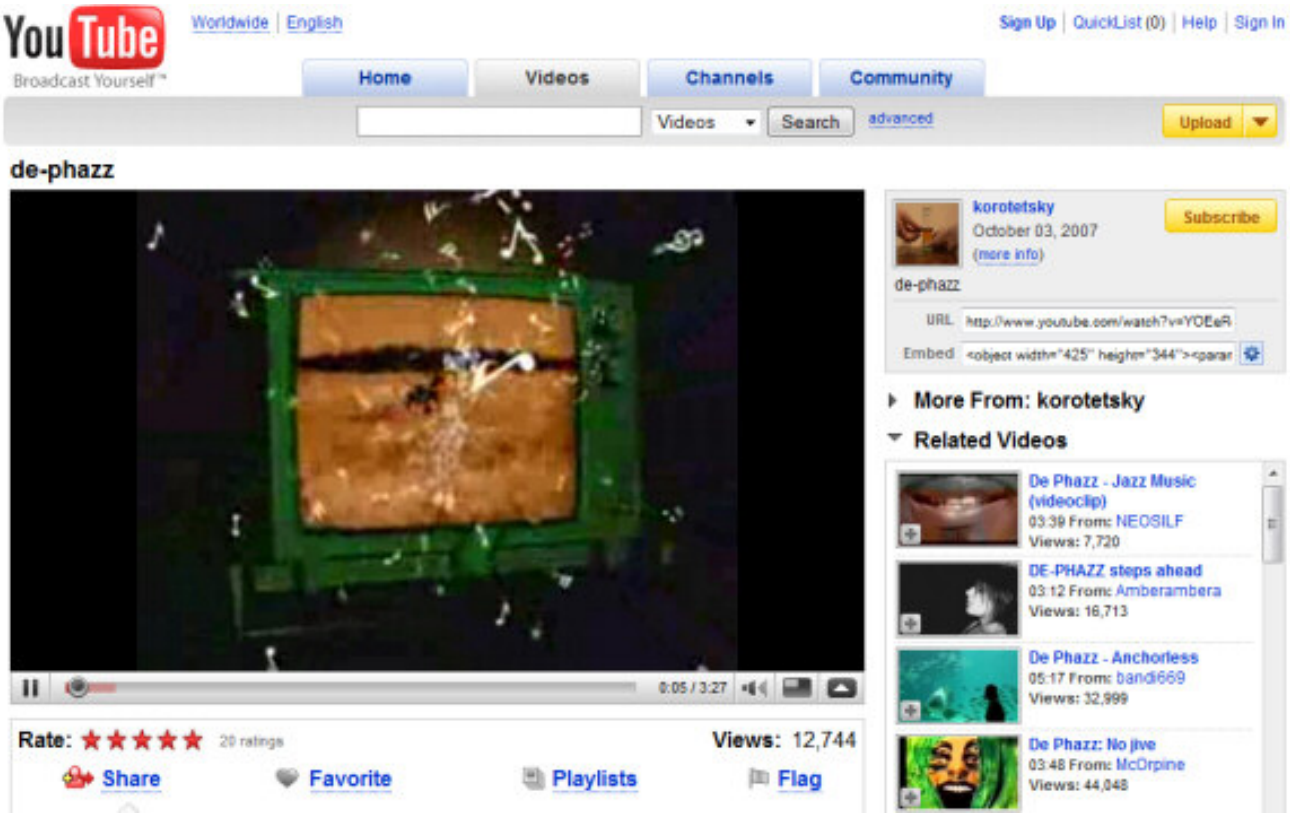
How Pakistan took down the mighty YouTube with one simple advertisement

"On the Internet, nobody knows you're a dog."

Weakness in Internet Routing

- Lack of Origin Authentication
  - Who own the IP address?
  - Who sent the packet?
- Route Hijacking
  - An arbitrary node/router originates a route for a range of IP addresses it does not own
  - Route is advertised to its neighbors via BGP
  - Propagated to the entire internet
  - Traffic is diverted from original destination

YouTube.com: 208.65.152.0/22



Pakistan blocks YouTube for 'blasphemous' content: officials

(AFP) – Feb 24, 2008

ISLAMABAD (AFP) — Pakistan has ordered all Internet service providers to block the YouTube website for containing "blasphemous" content and material considered offensive to Islam, officials said Sunday.

An inter-ministerial committee has decided to block YouTube because it contained "blasphemous content, videos and documents," a government official told AFP.

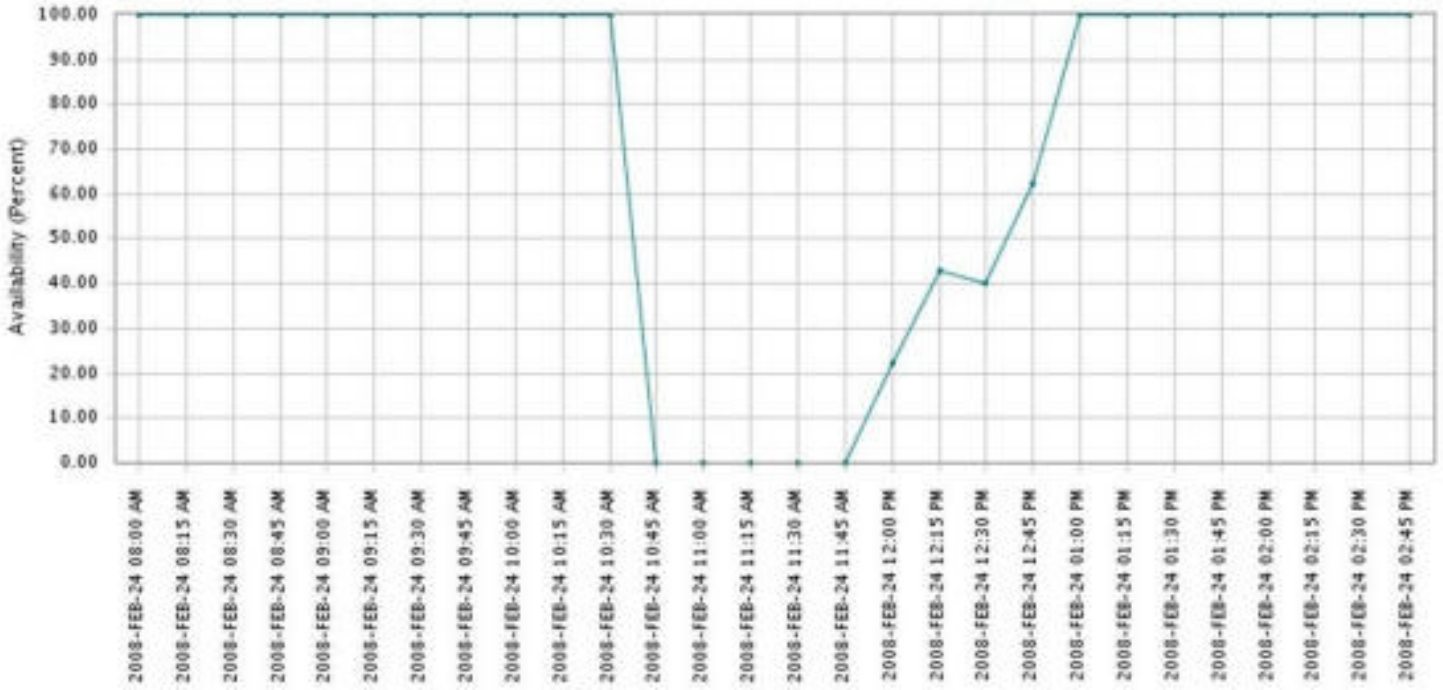
"The site will remain blocked till further orders," he said.

Other officials said the site had been blocked because it contained controversial sketches of the Prophet Mohammed which were republished by Danish newspapers earlier this month.

Sunday, 24 February 2008 18:47:00 UTC

- Pakistan Telecom Advertises 208.65.153.0/24
- This was leaked to its ISP, PCCW (AS 3491)
- PCCW (AS 3491) advertised this route to its neighbors …
- Recall YouTube is advertising 208.65.152.0/22
- What will happen?
  - Think of longest prefix matching!

YouTube Availability



Epidemic Spread

- 18:47:45 - First evidence of hijacked route propagating in Asia, AS path 3491 17557
- 18:49:00 - Several big trans-Pacific providers carrying hijacked route (9 ASNs)
- 18:49:30 - All providers who will carry the hijacked route have it (total 97 ASNs)

20:07:25 UTC

- YouTube, AS 36561 advertises the /24 that has been hijacked to its providers
- Does this solve the problem?

20:18:43 UTC

- AS36561 (YouTube) starts announcing 208.65.153.128/25 and 208.65.153.0/25.
- Because of the longest prefix match rule, every router that receives these announcements will send the traffic to YouTube.

20:59:39 UTC

- AS3491 (PCCW Global) withdraws all prefixes originated by AS17557 (Pakistan Telecom), thus stopping the hijack of 208.65.153.0/24

Event Timeline

18:47:00 Uninterrupted videos of Exploding jello
18:47:45 First evidence of hijacked route propagating in Asia, AS path 3491 17557
18:48:00 Several big trans-Pacific providers carrying hijacked route (9 ASNs)
18:48:30 Several DFZ providers now carrying the bad route (and 47 ASNs)
18:49:00 Most of the DFZ now carrying the bad route (and 93 ASNs)
18:49:30 All providers who will carry the hijacked route have it (total 97 ASNs)
20:07:25 YouTube, AS 36561 advertises the /24 that has been hijacked to its providers
20:07:30 Several DFZ providers stop carrying the erroneous route
20:08:00 Many downstream providers also drop the bad route
20:08:30 And a total of 40 some-odd providers have stopped using the hijacked route
20:18:43 And now, two more specific /25 routes are first seen from 36561
20:19:37 25 more providers prefer the /25 routes from 36561
20:28:12 Peers of 36561 start seeing the routes that were advertised to transit at 20:07
20:50:59 Evidence of attempted prepending, AS path was 3491 17557 17557
20:59:39 Hijacked prefix is withdrawn by 3491, who disconnect 17557
21:00:00 The world rejoices …

More Information on the YouTube Hijack

- http://news.cnet.com/8301-10784_3-9878655-7.html
- http://www.ripe.net/news/study-youtube-hijacking.html
- http://www.youtube.com/watch?v=IzLPKuAOe50
- http://abcnews.go.com/Technology/story?id=4344105

Route Hijacking

- https://en.wikipedia.org/wiki/IP_hijacking#Public_incidents
- Why does route hijacking happen?
  - 1. lack of origin authentucation
  - 2. misconfigured routers leaking unauthorized routes
  - 3. router update is on an “honor” system
  - 4. BGP was designed for efficiency, not security
- Can you prevent route hijacking?
  - Currently, the answer is NO.
  - Security is a major problem in the internet today.
  - We need good security policies and enforcement of those policies
  - Potential solutions: SecureBGP & Pretty Good BGP

How do countries block websites?

- http://news.asiaone.com/news/singapore/singapore-block-access-overseas-gambling-sites
- Many ways to block websites:
  - 1. Use DNS to block lookups (Black Hole)
  - 2. Advertise false routes (redirect to another page)
  - 3. Block the range of IP addresses (Black Hole)
- Can you bypass blocks?
  - Don't do it. The Government knows what is good for your soul!!
  - Or if you really need to, use vpn

Is this an isolated event?

- April 1997 - Black Hole Routing

https://en.wikipedia.org/wiki/AS_7007_incident

- Here is what happened:

http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html