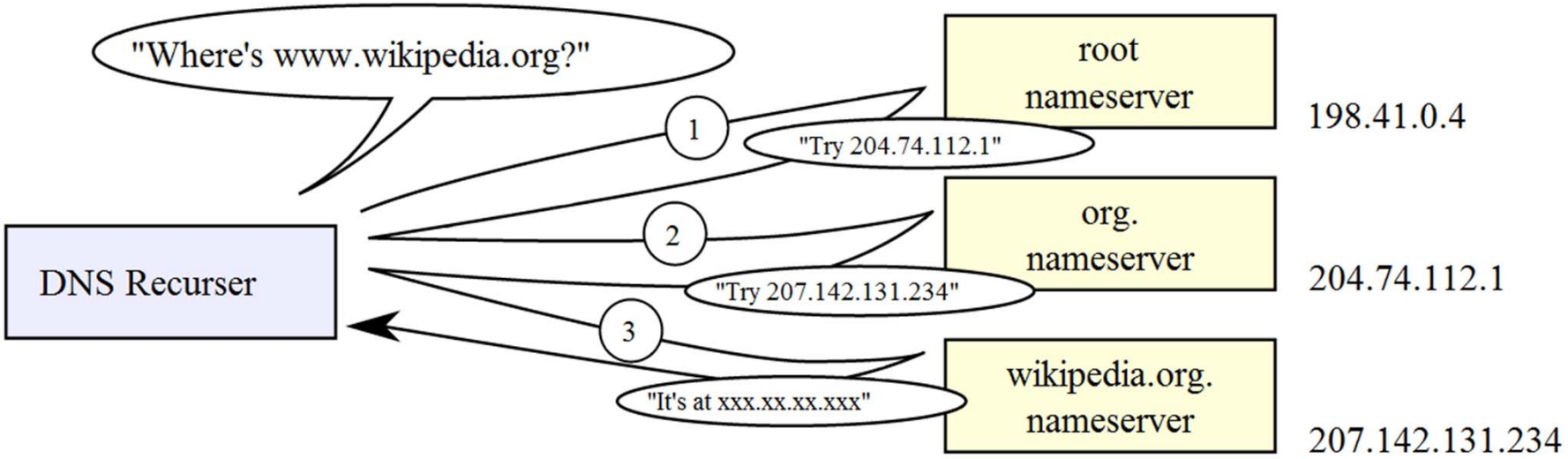
DNS Bitsquatting

Danny Cooper

What is DNS?

- Say we want to reach www.abc.com
  - Need to translate the URL into an IP address to actually fetch content
    - Make a DNS Query to a DNS Server
    - Receive a DNS response, containing the correct IP for the URL we requested.
  - How does the DNS Server resolve a URL?

Naïve DNS Resolution Example:



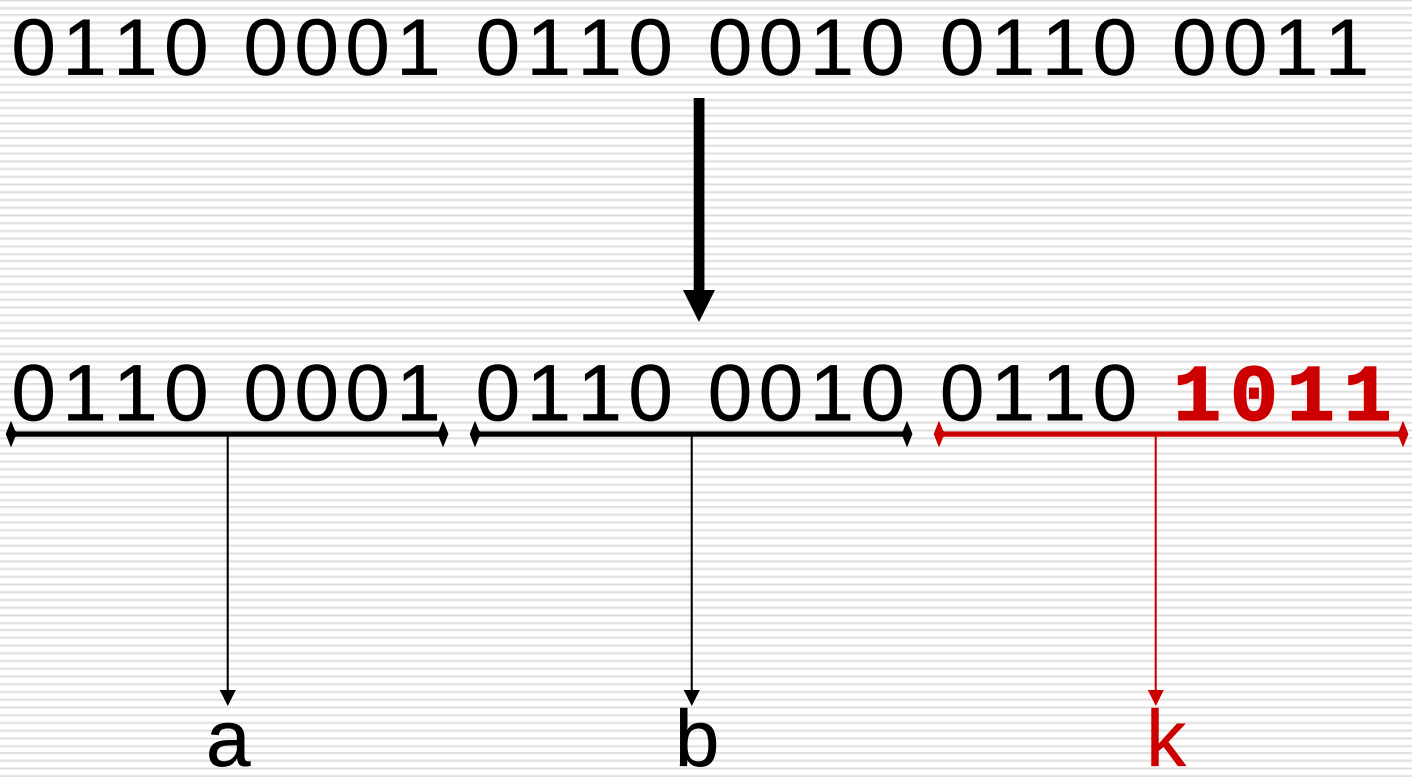
- Usually, however, we just use a cached answer

  - Image credit http://upload.wikimedia.org/wikipedia/commons/7/77/An_example_of_theoretical_DNS_recursion.svg

The Attack:

- Say we want to reach www.abc.com
- We do a DNS lookup
  - ~1500 DNS lookups made per user, per day (estimate from OpenDNS data)
- We character encode abc as:
  - A = 61 = 0110 0001
  - B = 62 = 0110 0010
  - C = 63 = 0110 0011
- What if a bit gets randomly flipped?
  - Known as a bit error, more on this later

Random Bit Flip Example:



The Attack (contd.):

- So, now we are asking for abk.com instead.
- What if a malicious third party registers abk.com?
  - Phishing
  - Code injection
  - Arbitrary Malicious Content

How it works:

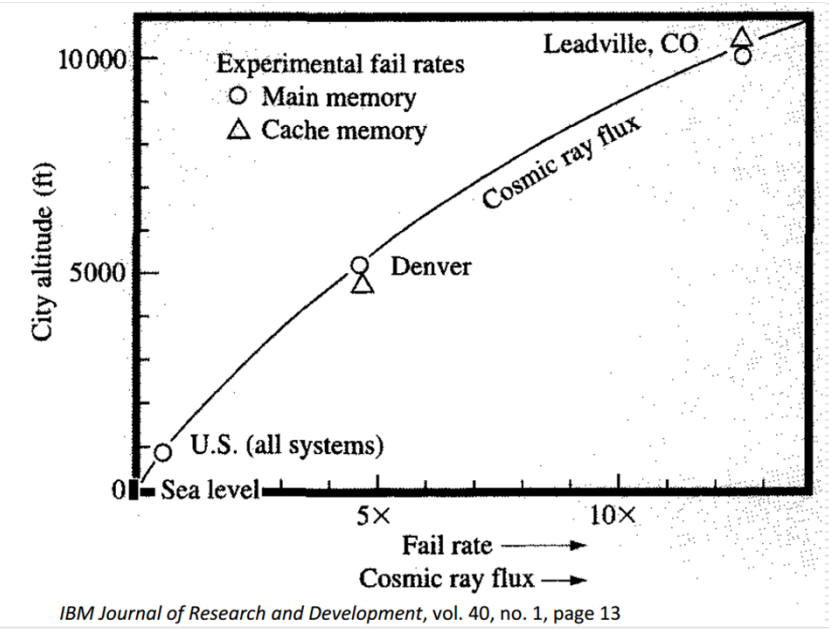
- We query for abc.com, but get abk.com's IP.
  - A bit error occurred *somewhere* in the DNS chain, probably locally.
- If abk.com's owner is malicious:
  - abk.com answers the http request, sending a response "from" both abc.com and abk.com
    - Needs to identify itself as being abc.com for request to go through.
  - We can now freely send content to the user, who thinks we are abc.com

Why This is Bad:

- Recall, ~1500 daily DNS lookups
  - Its even worse: ~1497 are not made directly by the user. (visualeconomics)
  - Requests for ads, content (CDNs), scripts, etc…
  - Your facebook session might be loading scripts from many different domains, each requiring resolution!
- Hardware vulnerability, not software

Why Bit Errors Happen:

- Cosmic Rays
- Extreme Temperature
- Poor manufacturing
- Power grid instability



IBM Journal of Research and Development, vol. 40, no. 1, page 13

How we can prevent bit errors:

- ECC Memory
- Preregistering squattable domains
- Designing site code to be aware of the possibility of squatting

Extensions and Implications:

- What if a bit error occurs at the DNS level and is cached?
- What if a bit error occurs in a webserver, causing it to serve html containing an erroneous URL?
  - This happened in a test case– Farmville was erroneously referring to squatted CDN domain, caused huge spikes.

Bibliography

- Dinaburg, Artem. "Bitsquatting DNS Hijacking without Exploitation." . Raytheon Company, July, 2011. <http://goo.gl/qoBfa>.
- Dinaburg, Artem. "Bitsquatting DNS Hijacking without Exploitation." . DEFCON, August, 2011. <http://goo.gl/4yyW7>.
- IBM Journal of Research and Development, vol 40, no. 1, page 13

  http://goo.gl/UAFuo
- “DNS Protocol”. Microsoft Technet <http://goo.gl/2YttV>
- Image credit: LionKimbro <http://goo.gl/nKuyk>