ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

Information-Centric Networks

Section # 3.1: DNS Issues

Instructor: George Xylomenos

Department: Informatics

European Union
European Social Fund

OPERATIONAL PROGRAMME
EDUCATION AND LIFELONG LEARNING
investing in knowledge society
MINISTRY OF EDUCATION, LIFELONG LEARNING AND RELIGIOUS AFFAIRS
MANAGING AUTHORITY

NSRF 2007-2013
programme for development
EUROPEAN SOCIAL FUND

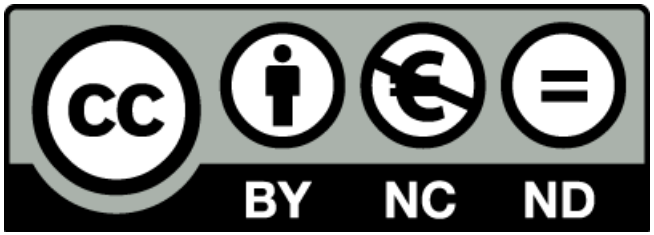
Co- financed by Greece and the European Union

Funding

- These educational materials have been developed as part of the instructors educational tasks.
- The **“Athens University of Economics and Business Open Courses”** project only funded the reformatting of these educational materials.
- The project is being implemented as part of the Operational Program “Instruction and Lifelong Learning” and is co-financed by the European Union (European Social Fund) and national funds.

Licencing

- These educational materials are subject to a Creative Commons License.



Directory services

- Browser autocompletion misuses DNS
  - As you type, your browsers guesses what you want
  - This requires DNS queries as you type
  - Of course they only query for valid looking names
    - They will not look for w, ww, www, www.c
    - But they will look for www.cn and www.cnn.co
    - One in China, one in Colombia!
  - Essentially, this is using the DNS as a directory service
  - If DNS was designed to do this, it would reverse names
    - com.cnn.www rather than the other way around
    - This walks the name tree in the right order
  - At least this should be made optional
    - We can then argue whether it should be opt-in or opt-out

Week 3 / Paper 1

- What DNS is not
  - Paul Vixie
  - CACM, December 2009, vol. 52, no. 12
- Main point
  - “DNS is many things to many people – perhaps too many things to too many people”
  - The DNS is essentially a hierarchical distributed database
  - The goal of DNS is to translate names to addresses
  - But currently the DNS is used in many other ways
  - Why is it bad to use the DNS in other ways?

DNS use and misuse

- The DNS is critical for the Web
  - Every Web page view starts with a DNS transaction
    - Translate server name to IP address
- Monetized intermediation
  - A common misuse of the DNS is redirection for profit
  - You ask for an address and instead get an ad page
  - Someone makes money out of this redirection
- DNS is not a directory system
  - Directory systems approximately answer approximate questions
  - DNS only exactly answers exact questions
  - Misusing the DNS this way has a cost for everyone

Stupid DNS tricks

- DNS lookups misused as mapping requests
  - CDNs use lookups to redirect web browsers
  - The IP of the source is used to select a content server
  - Based on server load and proximity to the client
- What does this mean for DNS?
  - Caching is prohibited to allow answers to change
    - Normally the TTL of replies is very low
  - And it may not even lead to good decisions
    - DNS requests can be recursive
    - The source IP may not have much to do with the client
    - Lots of tricks are needed to provide good answers
  - DNS server load is increased for everyone
    - But it does not affect the CDN operator's revenue!

NXDOMAIN remapping

- NXDOMAIN is returned for non-existent domains
  - Due to mistyping or software/hardware failures
  - These answers can be cached like all other answers
  - Applications treat NXDOMAIN as an error
    - Error pages, bounced e-mails, server does not exist
- Returning ad pages instead of NXDOMAIN
  - Instead of an error, you get a web page
    - The DNS is lying for money
  - Applications cannot determine that an error occurred
    - Web clients can because a human sees the response
  - Widespread practice in third party DNS servers
  - Some ISP block these servers to do this trick themselves!

Damage control

- NXDOMAIN remapping has many implications
- Cookies use the same origin trust model
  - You can send a cookie to the domain you got it from
  - Say that you misspell a server name but not the domain
  - The ad server may receive your cookie for that domain
- MX entries can also be redirected
  - Your e-mail will end up in an ad server
  - In theory MX records are not remapped
    - But there is no foolproof way to do this
- Standard bad practices
  - There is even an IETF proposal on how to lie consistently!
  - It breaks DNSSEC, but who cares?

A rescue being thought of

- The emergence of DNSSEC may stop such problems
  - DNSSEC allows zone info to be signed and verified
    - Using public key cryptography
  - Private keys are held by authoritative servers
  - Public keys are published in DNS
- DNSSEC can stop DNS lying
  - NXDOMAIN remapping returns invalid records
    - They do not come from the authoritative servers
  - Server redirection is not prevented
    - CDNs work with the content publishers
  - This is not why DNSSEC was designed
    - But it does the trick

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

End of Section # 3.1

Course: Information-Centric Networks, **Section # 3.2: DNS Issues**

Instructor: George Xylomenos, **Department:** Informatics

European Union
European Social Fund
OPERATIONAL PROGRAMME EDUCATION AND LIFELONG LEARNING
investing in knowledge society
MINISTRY OF EDUCATION, LIFELONG LEARNING AND RELIGIOUS AFFAIRS
MANAGING AUTHORITY
NSRF 2007-2013
programme for development
EUROPEAN SOCIAL FUND
Co- financed by Greece and the European Union