Study on **OS Fingerprinting** and NAT/Tethering Based on **DNS Log Analysis**

Deliang Chang <chdlgs@gmail.com>

Qianli Zhang <zhang@cernet.edu.cn>

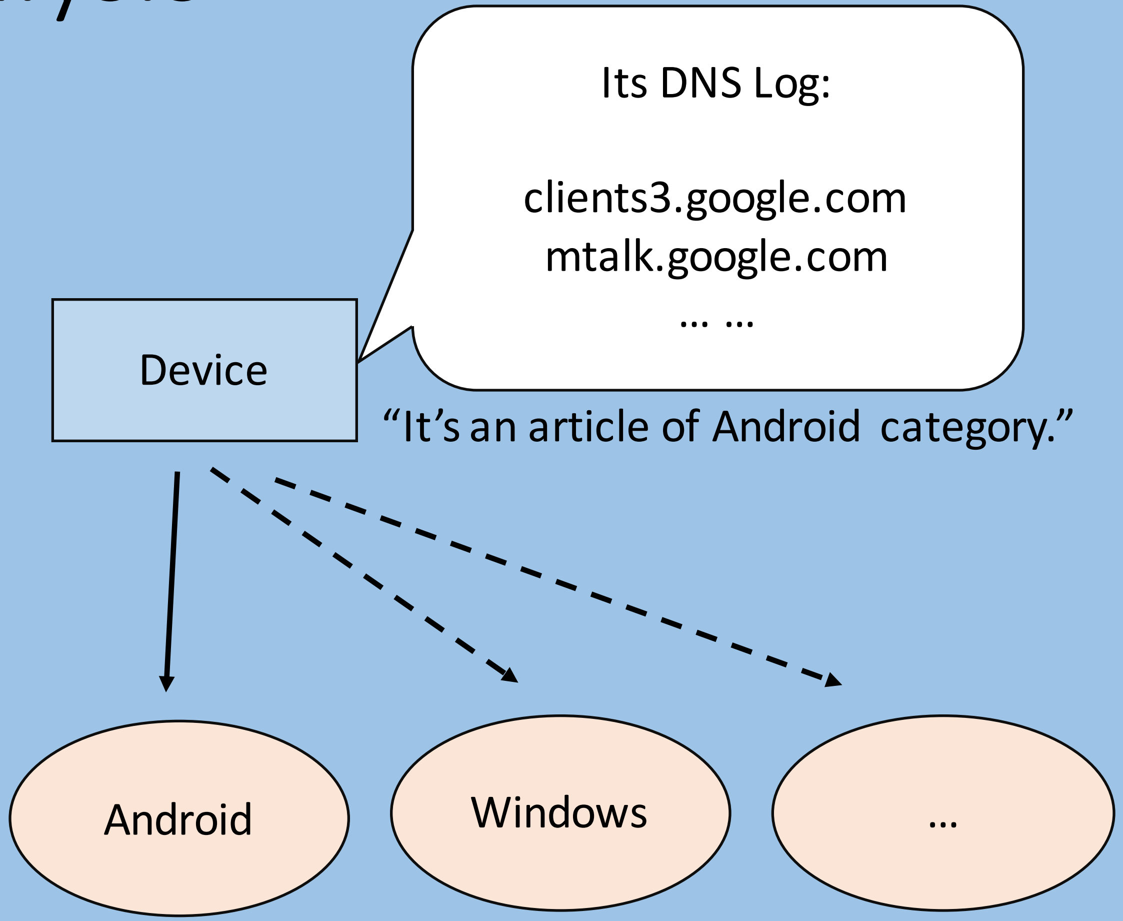
Xing Li <xing@cernet.edu.cn>

Study on OS Fingerprinting and NAT/Tethering Based on DNS Log Analysis

- Why DNS?
- Study on OS/NAT usage in our large-scale network(peak number of IP is more than **40000**).
- Many previous methods based on traffic analysis required TCP/IP headers or raw packets.
    - Gateway management required.
    - Raw packets' capture and store is difficult when facing to a large-scale network.
- DNS can be provided by either network administrators or third-party providers. Its log is also easier to store and examine.

Study on OS Fingerprinting and NAT/Tethering Based on DNS Log Analysis

- Modern operating systems may use os-specific DNS queries to implement tasks or have some os-specific applications.
- Borrow the concept of text categorization.
  - A device -> An article
  - A domain name -> A word
- Feature selection, classification…
- Good accuracy (**>90%**).



Its DNS Log:

clients3.google.com
mtalk.google.com
… …

"It's an article of Android category."

Study on OS Fingerprinting and NAT/Tethering Based on DNS Log Analysis

- Devices of different OSes online at the same time indicates NAT behavior.

- Even most mobile devices has hot-spot function to share connection with other device, people in China prefer to use laptops/PCs as hot-spots.
- The global IP address is enough in our network, but there’re still many devices choose to use NAT. Besides saving one or two IP addresses, sharing connection conveniently and quickly is another purpose.