Identity Trail: Covert Surveillance Using DNS

http://saikat.dyndns.org/pet07.pdf

Saikat Guha and Paul Francis

Cornell University

7th workshop on Privacy Enhancing Technologies

Where in the world is Paul Francis?

Meeting at 3 pm . . .

- San Jose
- Italy
- Cancun?!!

Identity Trail

Covertly keeping tabs on your advisor, or student, or employee, or spouse . . .

Identity Trail

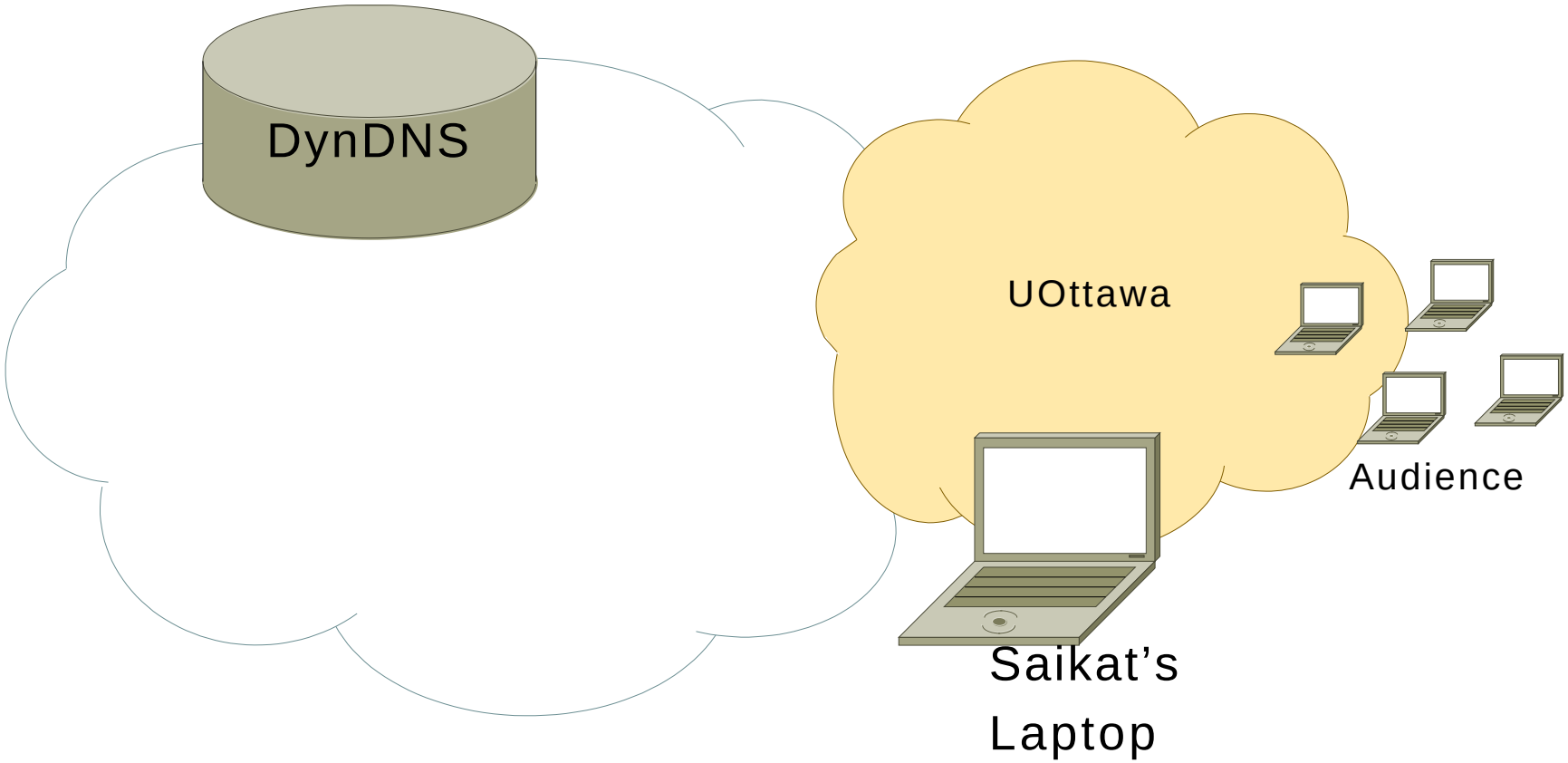
- Track someone without them knowing
  - Using public services (DNS, DynDNS, GeoIP)
  - Used like they were meant to be used
- Exploits
  - Public nature of DNS
  - Information derived from IP addresses over time
- Demonstrated for over 100K hosts
- Need for a new Internet naming architecture for non-public hosts

DNS and Dynamic DNS

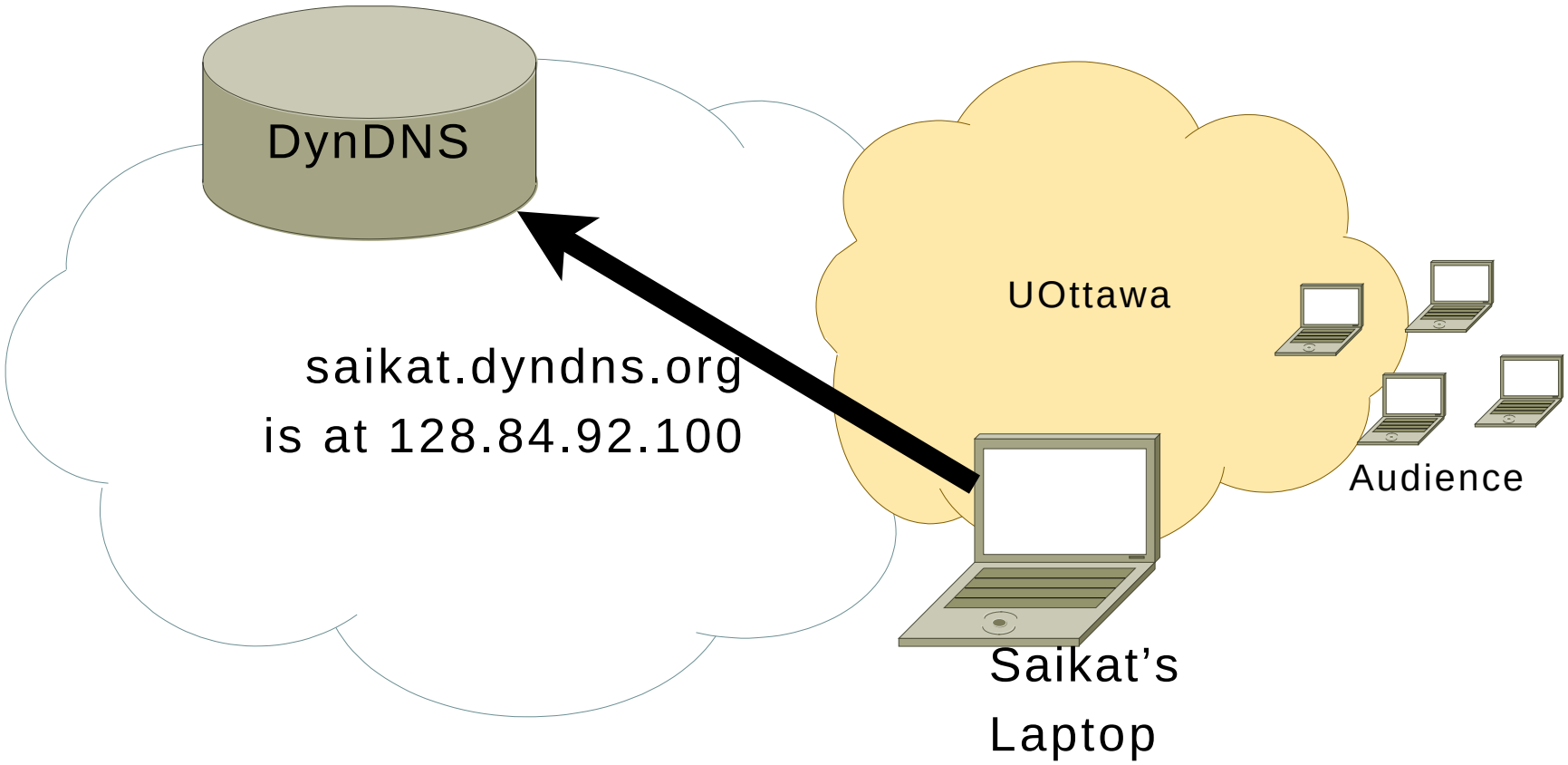
- DNS — Name to IP address mapping
  - All data public, privacy not considered
  - Envisioned for IP renumbering of fixed hosts
  - Occasional updates, by network admin.

- Dynamic DNS — More frequent updates
  - Envisioned for fixed hosts with DHCP addresses
  - Host updates third-party DNS server
  - Still public, privacy still not considered
  - (Ab)used by mobile hosts
    - No real alternative

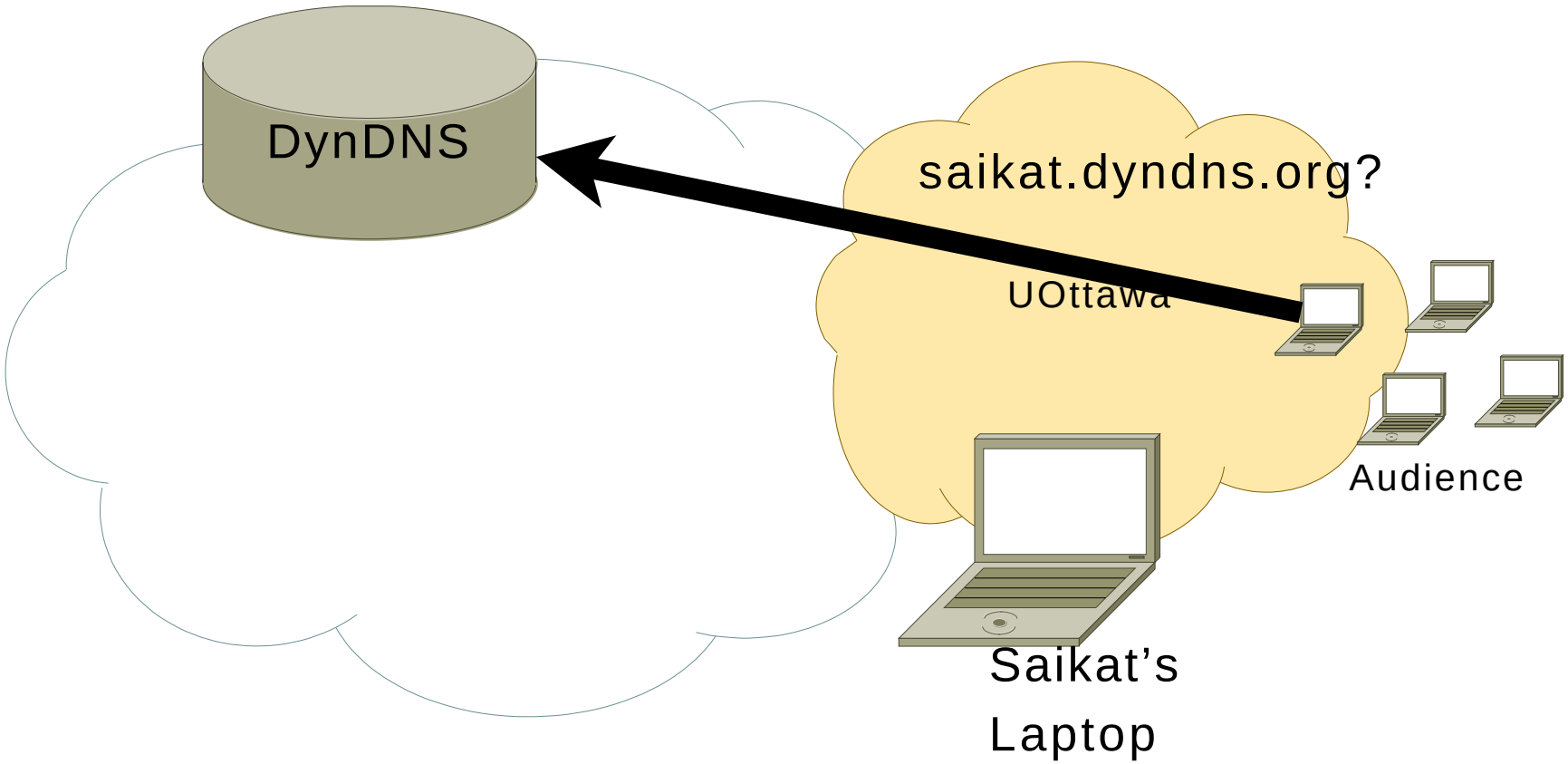
DNS: No access control



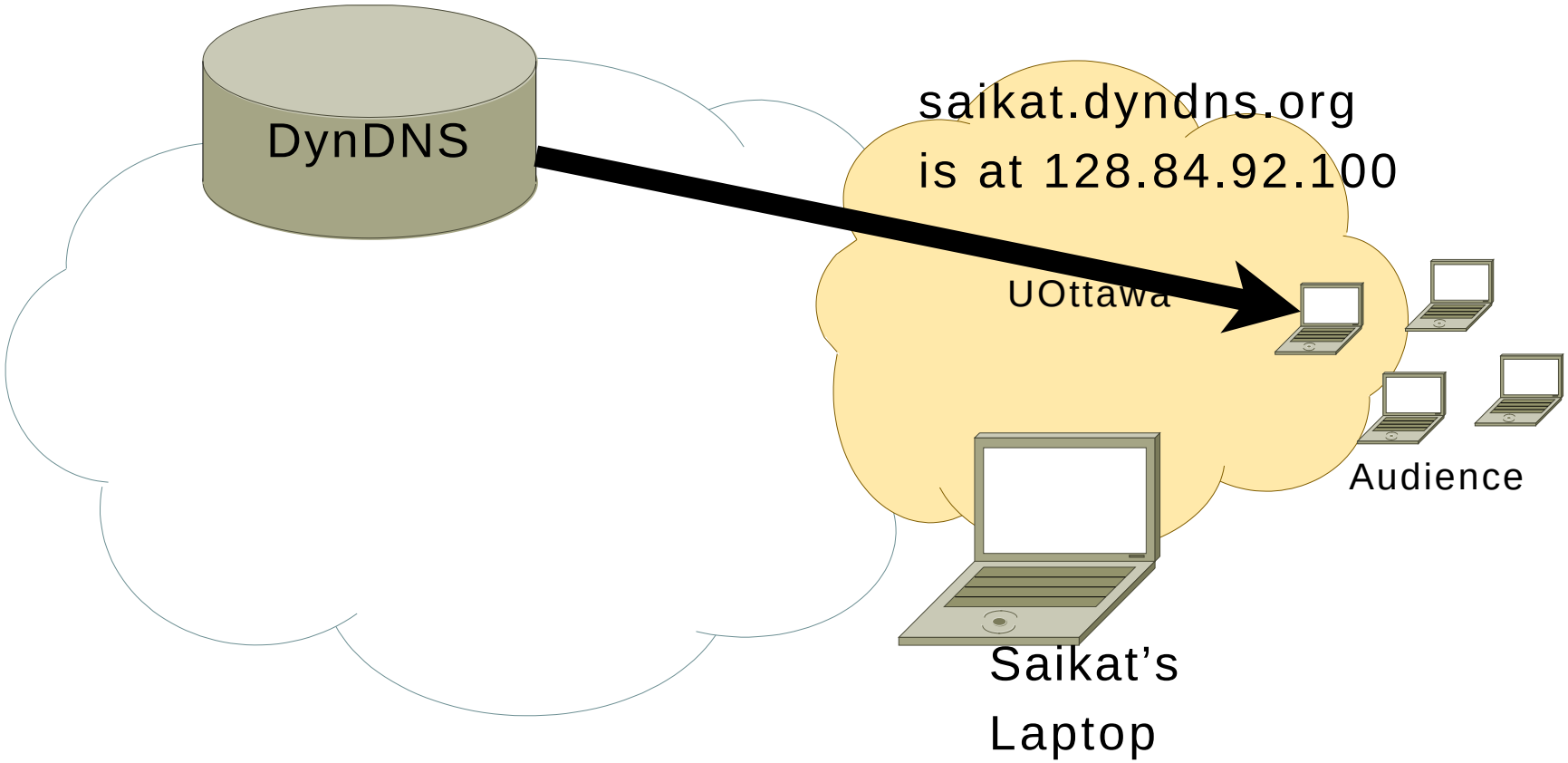
DNS: No access control



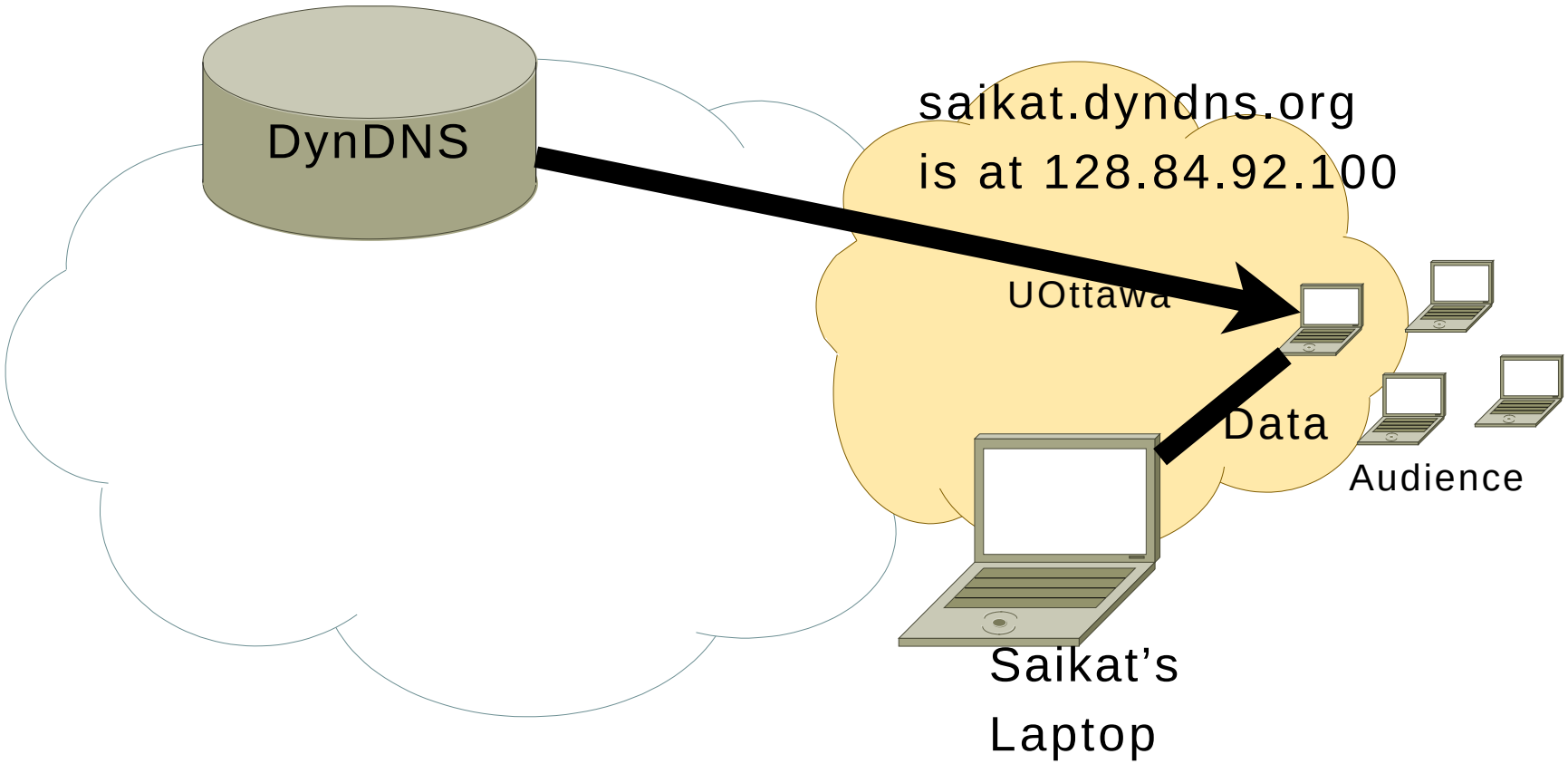
DNS: No access control



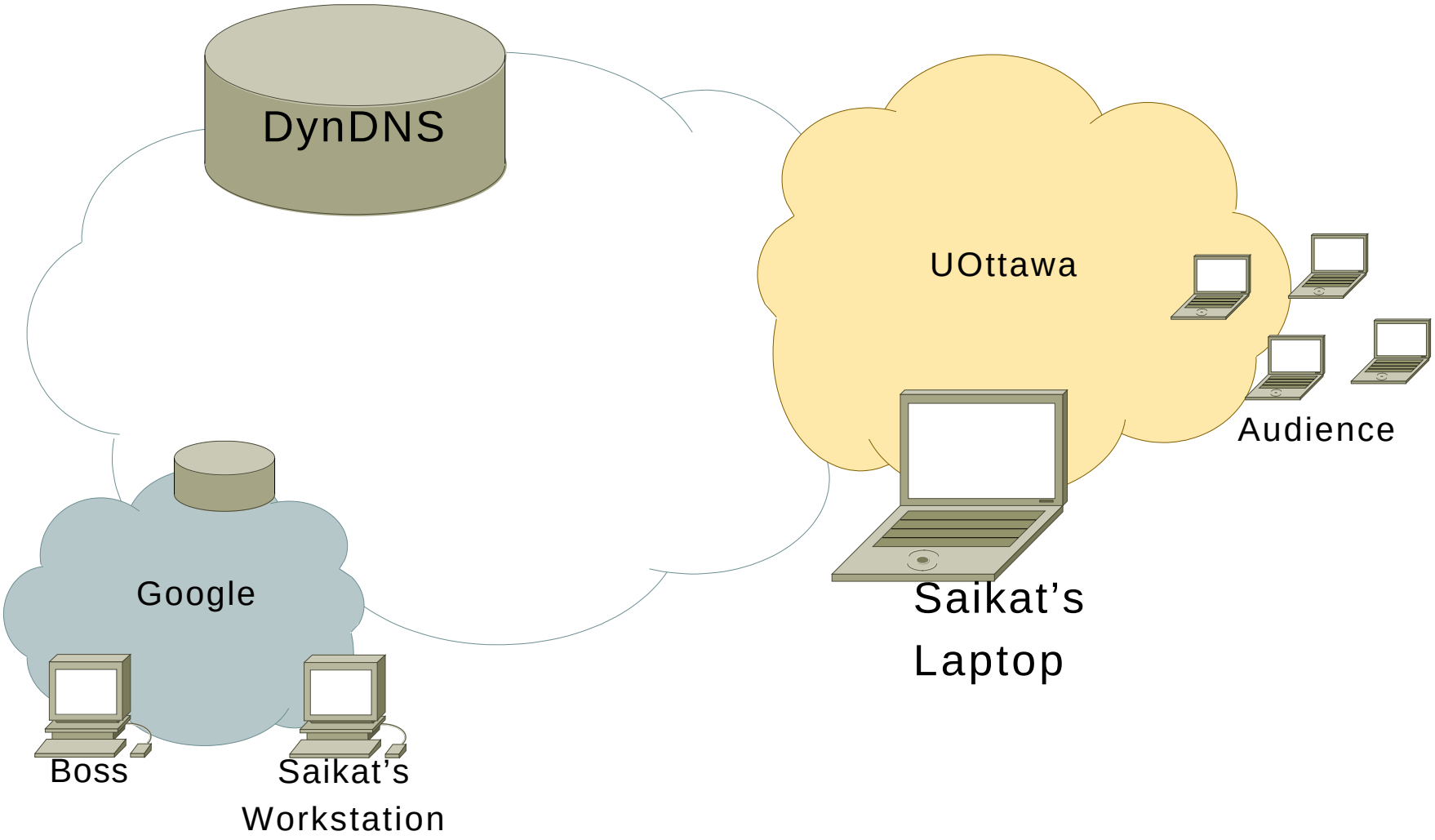
DNS: No access control



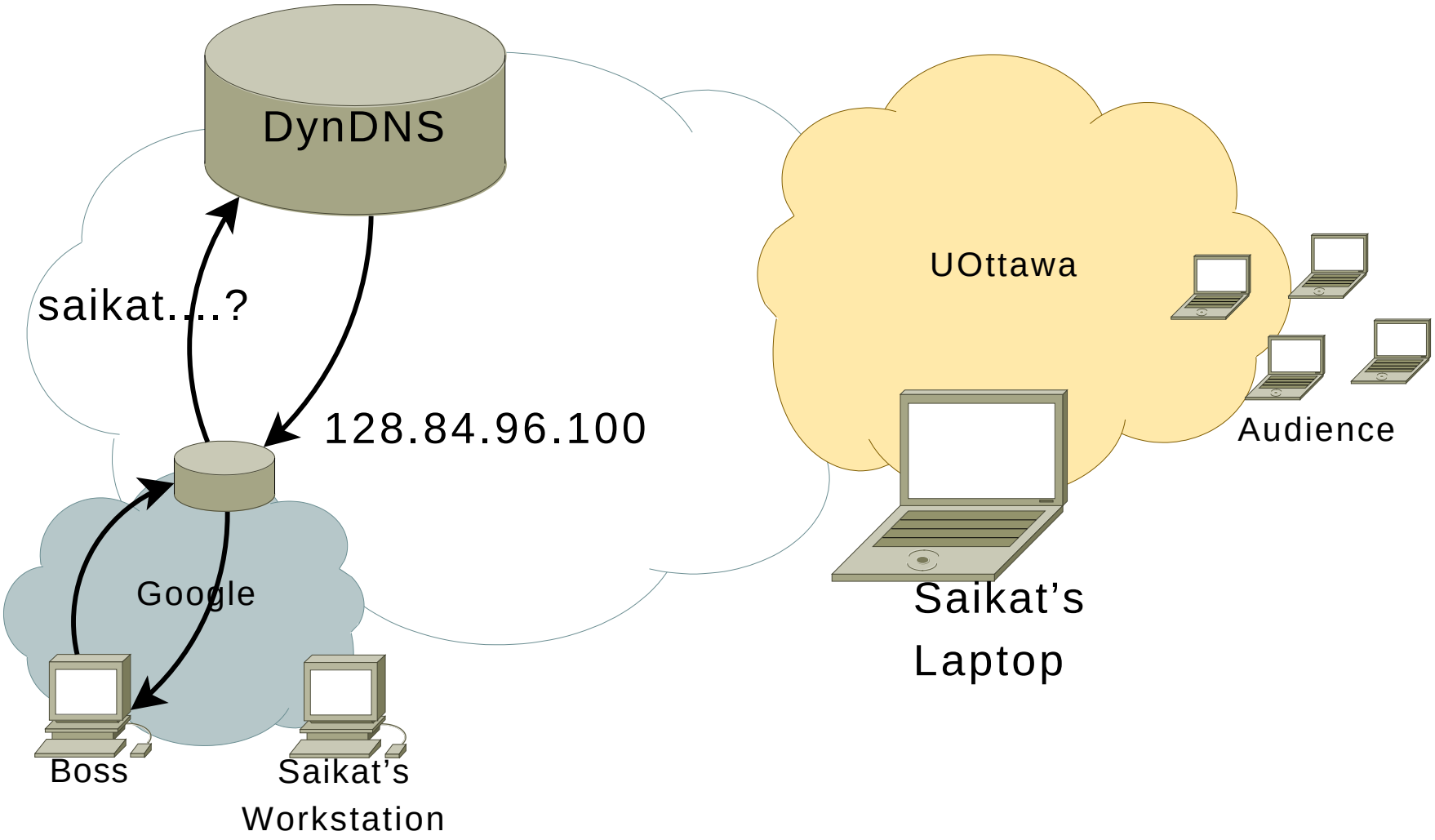
DNS: No access control



DNS: No access control



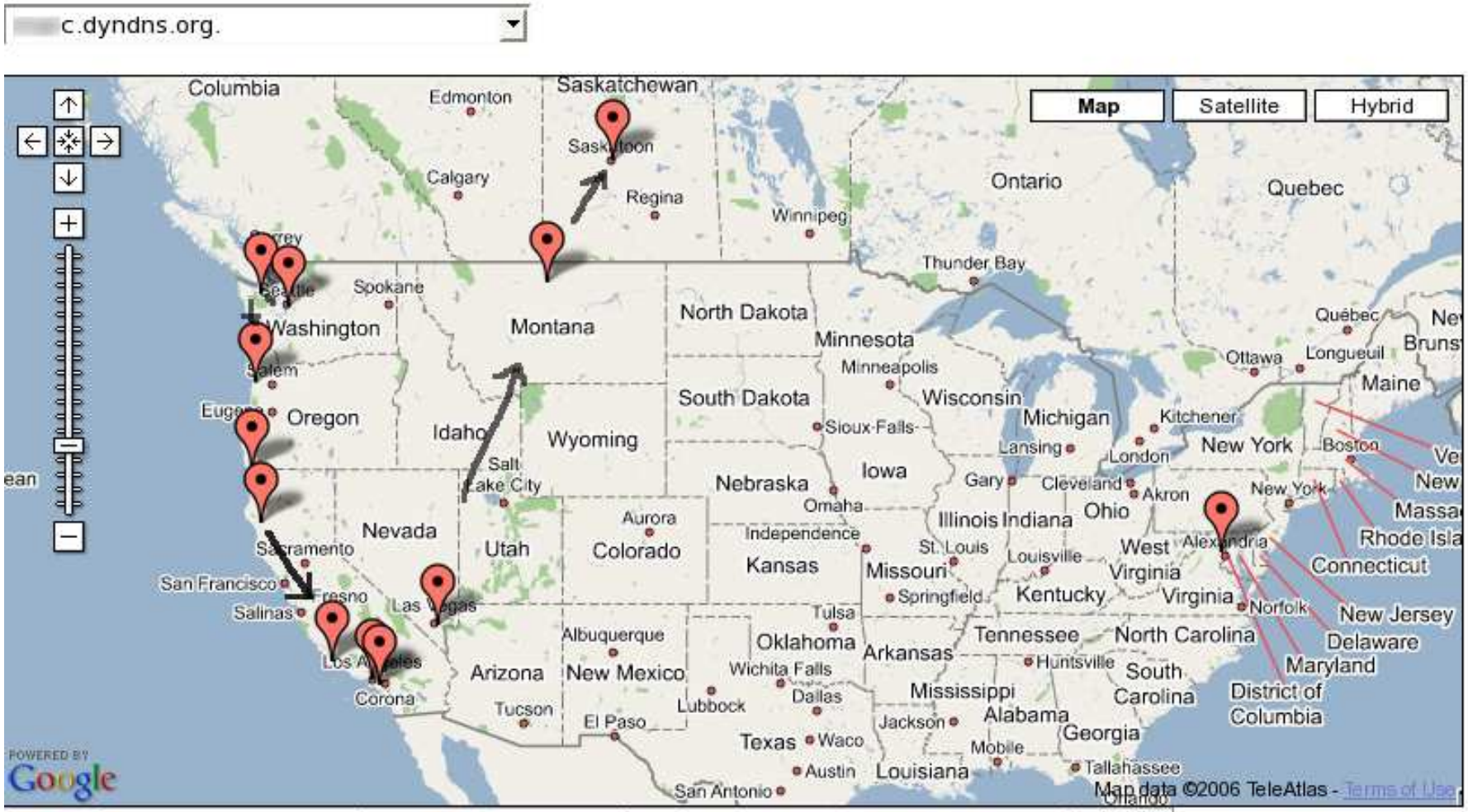
DNS: No access control



Identity Trail "Attack"

1. Find DNS hostname for victim
2. Perform DNS queries (Victim doesn't learn of query.)
3. Geo-locate IP address
4. Create dossier over months

That simple? Yes.



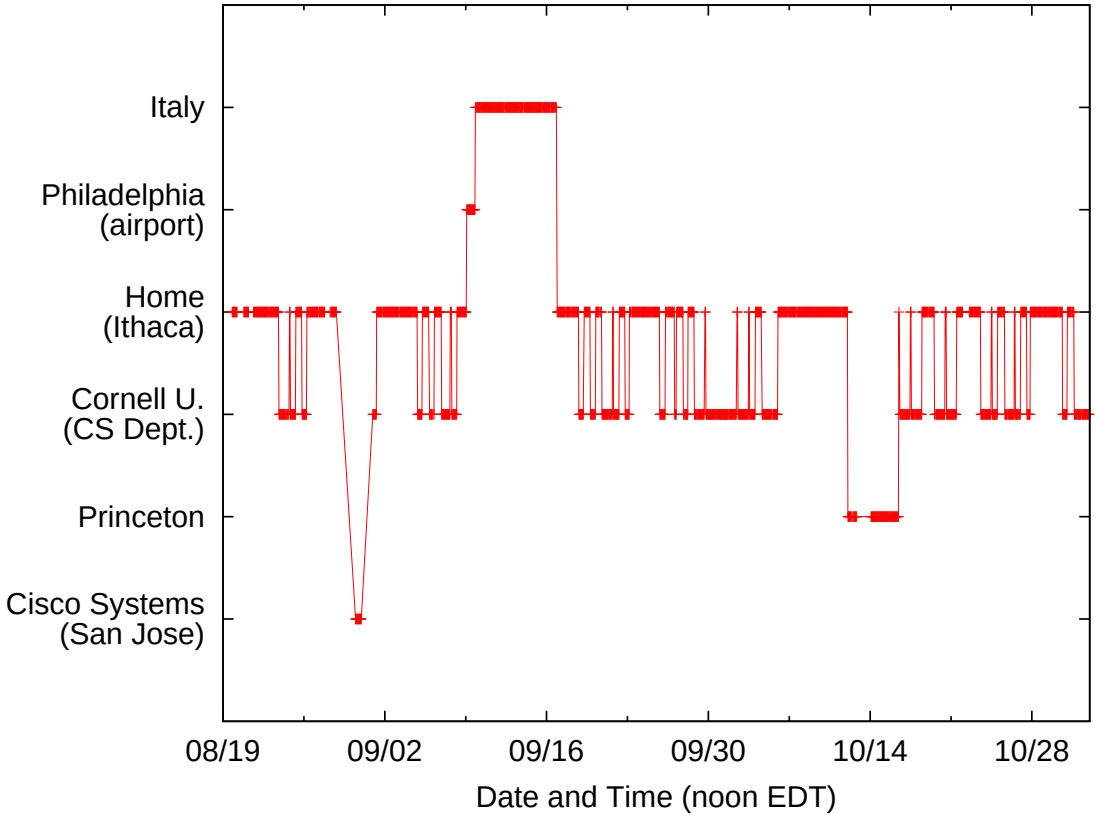
Date	ip	Block	Location	AS
Jul 20	24.[redacted]	24.22.192.0/18	Seattle, Washington, US	33650
Jul 20	24.[redacted]	24.22.192.0/18	Seattle, Washington, US	33650

Validation: Finding Victims

- Decided to target DynDNS users
  - Not the intended attacker model per se
- Google, Yahoo searches: surprisingly few (∼4K)
- Dictionary attack: many many more (∼31K)
- Nmap scan of a small number of victims
  - Services required authentication
  - Empty public landing pages etc.

DynDNS hostnames rarely advertised publicly. Most likely intended for private use.

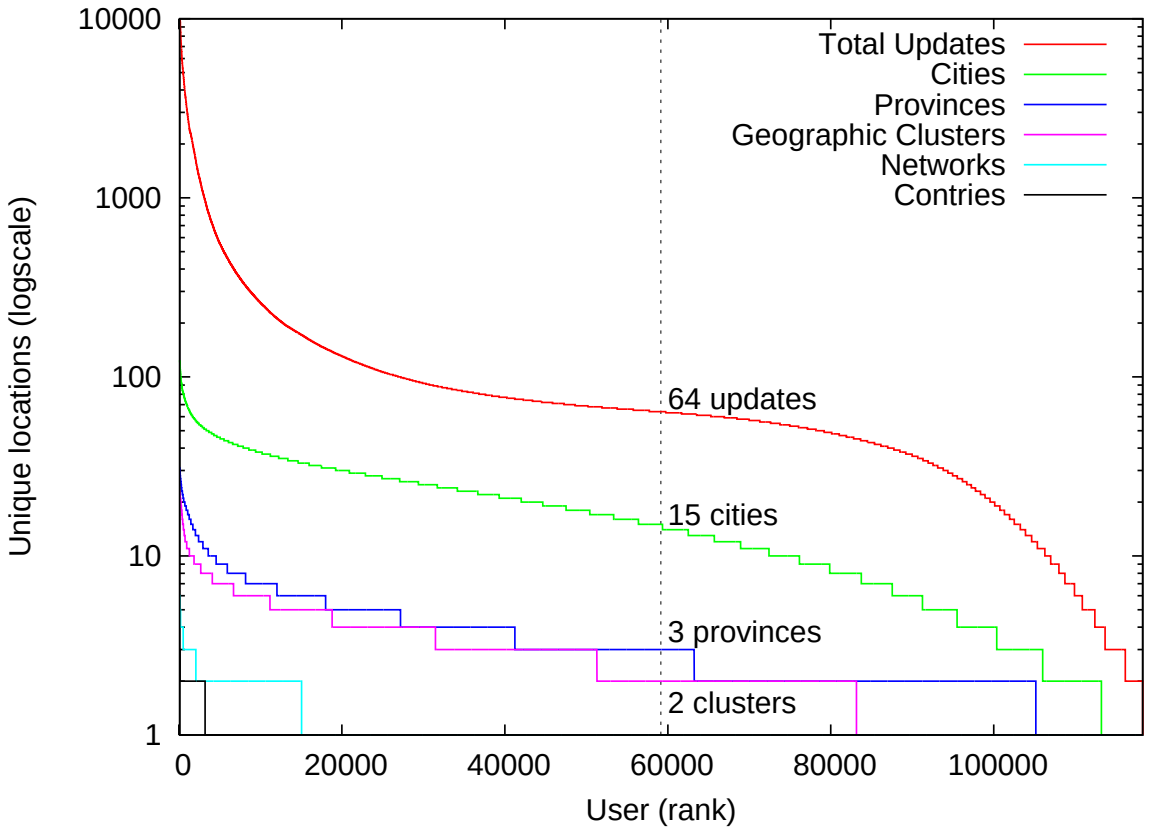
Validation: Accuracy



- Trailed Paul
- City-level accuracy in US (∼100 mi), province-level in Italy for GeoIP service used.
- Commute time accurate to within query interval. Some exceptions.

Reasonably good accuracy. Reconstructed travel itineraries, daily commute patterns.

Validation: Mobility



∼70% of the 125,000 DynDNS users trailed logged in from different locations. Disclaimer: data was noisy, see paper.

There exist many mobile users that want user-friendly name resolution for private services.

(Non)-Solutions

- Don't use DNS for mobile private hosts
  - Try `http://saikat.dyndns.org` now!
    (you will connect to this laptop. Imagine doing the same in IPv6 without DNS)
- Use a proxy like Akamai
  - No service for individuals. Operating costs.
- Encrypt IP addresses in DNS
  - Key management headaches

End-Middle-End Name Resolution

SIP animation here

Summary

FIXME

`http://nutss.net/`