Anonymity

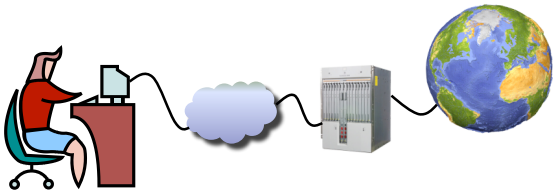
Datakom II course topic

Spring 2005

Outline

- What do we mean by anonymity?
- Technical solutions for anonymity
- Legal aspects

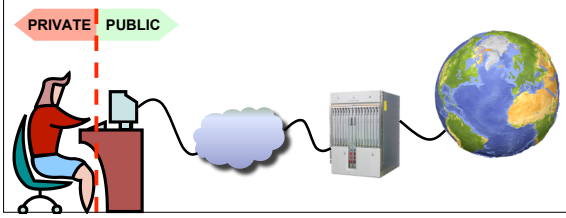
What do we mean by anonymity?



- Total anonymity can not be achieved
- The question is where to place the cut between public and private domain

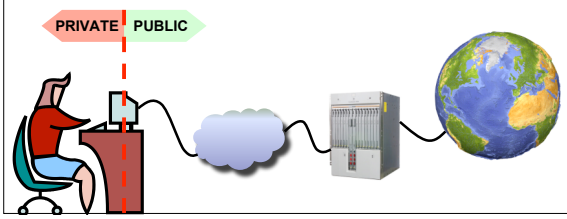
Placing the cut (1)

- Computer identity and potentially other details about the computer are known
- Identity of user unknown



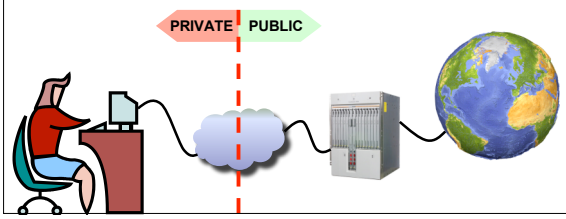
Placing the cut (2)

- Computer identity (IP) is known
- Details about computer and user are unknown



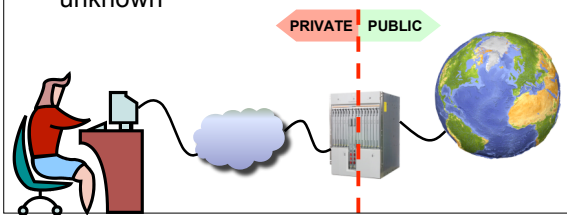
Placing the cut (3)

- LAN identity (IP subnet) is known
- Exact computer identity unknown, as are computer and user details



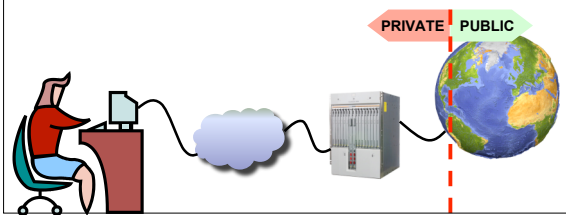
Placing the cut (4)

- AS (Usually second-level domain) is known
- Subnet, Computer and User details unknown



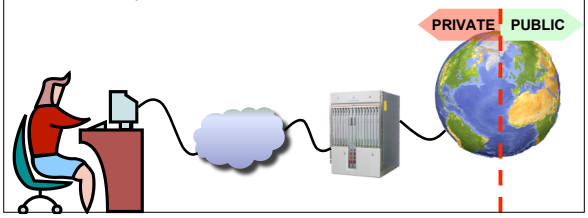
Placing the cut (5)

- Forwarding router is known
- Nothing is known about actual AS, IP, computer or user details



Placing the cut (6)

- Virtually nothing is known
  - Except maybe that the user is located on earth
- Is this possible to achieve at at all?



Where is the cut located?

- Previous sequence of slides ideal cuts
  - Some would call it naïve
- In most systems, the cut moves due to
  - Applications with different security models
  - Users with different security awareness
  - System administrators (and their mistakes)

What is ”the cut” ?

- A translator or protector between public and private domain information
- Examples of cut implementations
  - A NAT box for a large set of users
    - Like UPUNET-S
    - ”We know it is one of the students, but not whom”
  - A software-based firewall
    - Often serves to protect computer-internal data
  - An anonymizing webproxy
    - Hides the true identity of who is visiting a web page
- Information to protect often available ”in” the cut
  - Hack into the cut and anonymity is lost
  - More important: Someone can always(?) find out…

Technical focus of this course topic

- ”Pseudonymity”
  - Anonymizing your computer identity
    - Act under a consistent pseudonym
    - Not only aggregating it into LAN or AS
- Several principles exist…
  - Anonymizing proxies
  - Indirection infrastructures
  - Onion routing
  - Data dissemination techniques

”On the Internet, nobody knows you’re a dog”

One slide about cuts close to user

- To secure information in your computer
  - Use a firewall
  - Use antivirus software
  - Update your OS periodically
    - Windows XP users – free license available!
- To protect information in your computer
  - Cryptographical file systems
- Anxiety at a destructive security intrusion directly proportional to backup interval

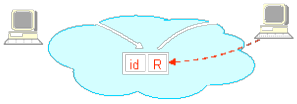
Proxy-based solutions

- No direct connection to destination
  - Connections relayed by a proxy
  - It appears like the proxy is the source
  - In fact, this is what a NAT box basically does
- Mapping between proxy ID and true ID
  - Usually stored in a table in the proxy
  - How well do you trust the proxy admin?

Chained proxies

- Doing the proxy trick twice (or more)
  - Several anonymizing proxies are out there
  - From the first, connect to another one
    - …and so on
  - Makes it harder to reverse-map proxy state to real user identity
- Some proxies prevent this
  - One might ask why…

Indirection infrastructure (i^2)



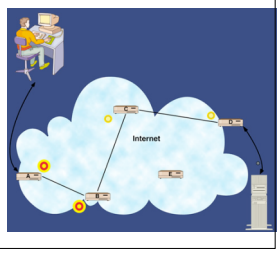
- Basic operation
  - Don't use IP addresses as identifiers
  - Servers mapped into service identifiers
  - A client connects to a service identifier
    - Indirection infrastructure act as a distributed proxy
    - Client and server may not be aware of each others identities
- Exists in some different forms
  - Established indirection infrastructures
  - Peer-to-peer based indirection infrastructures

I^2 drawbacks

- Clients and servers must be I^2-aware
  - Makes global deployment cumbersome
- Information control in distributed systems
  - Can be hard to ensure who is knowing what
    - Especially to guarantee that X does not know Y
- Mapping between IP/FQDN and service ID:s
  - What should service ID:s look like?
  - Several proposals (too many chefs…)

Onion routing

- Similar to chained proxies
  - The onion routers form an *onion cloud*
- Proxy chain randomly selected
  - On per-flow or per-packet basis
  - Hidden to end hosts
- Also similar to I^2
  - …but without a separate naming space



Onion routing - drawbacks

- Who is in the onion cloud?
  - For P2P-based clound, problem even tougher
- Delay variations
  - If paths are selected on per-packet basis
  - Could penalize protocols like TCP…
- Vulnerable to certain attacks
  - Intersection, predecessor…

Data dissemination

- Most usable for popular data
- Data ”flows” in network
- Usable in multi-hop sensor networks
  - …can also be used in high-speed networks
  - …or to achieve anonymity
    - If interested in data, save a local copy

Student seminar

- A closer look at technical solutions
- Sign-up on sheet
- Topics assigned after next lecture

Next lecture

- ”Softer topics”
  - The why:s of anonymity and pseudonymity
  - Legal aspects
    - Discussion topic
  - The feasability of an anonymous Internet