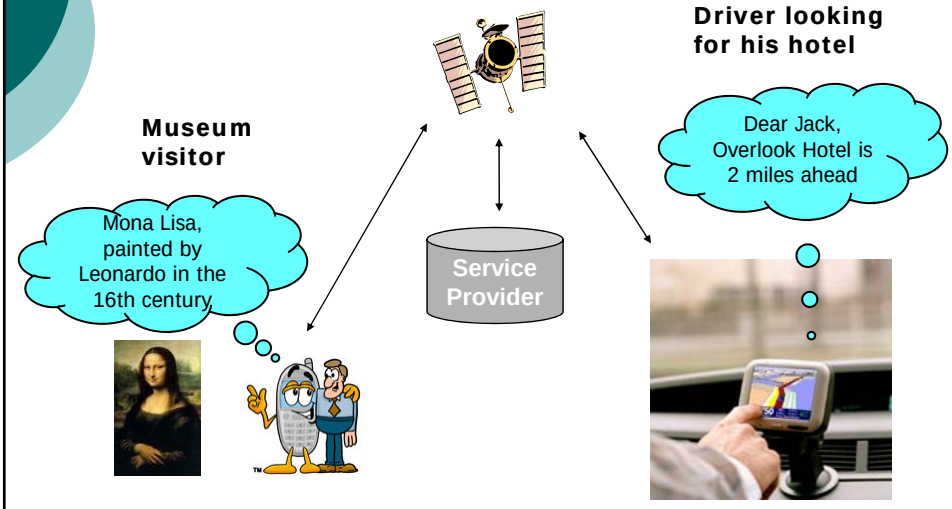
Privacy in Last-Hop Wireless

Location-aware services



Threats

- Communication Data Privacy
  - What data is being sent?
- Communication End-point Privacy
  - Who is the sender of the message?
- Location Privacy
  - Who (perhaps unknown) is moving where?
  - Knowledge of visited locations (tracking) can provide clues about private information, e.g., political affiliation, alternative lifestyle, or medical problems/issues

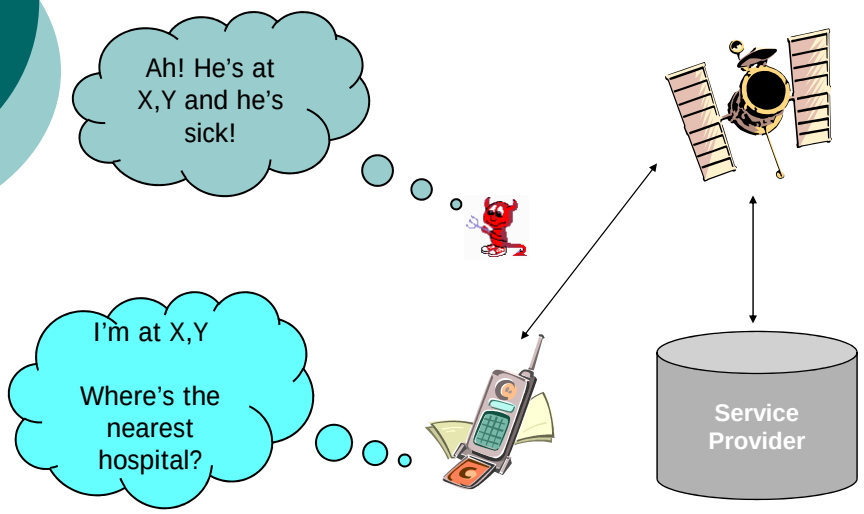
Different levels of location privacy

- Location-based Services
  - Locate a user in a city, street, building
  - Discrete sampling
    - Possible only if user requests the service
- WLAN
  - Locate a user in a room
  - Continuous Sampling
    - Track user movements over time

K–anonimity

- Key concept in many solutions to location privacy
- Informally, information is said to satisfy **k–anonymity** if it is “linked” to at least k individuals (entities)
- Equivalently, adversary cannot link any message to < k entities

Location-Based Services



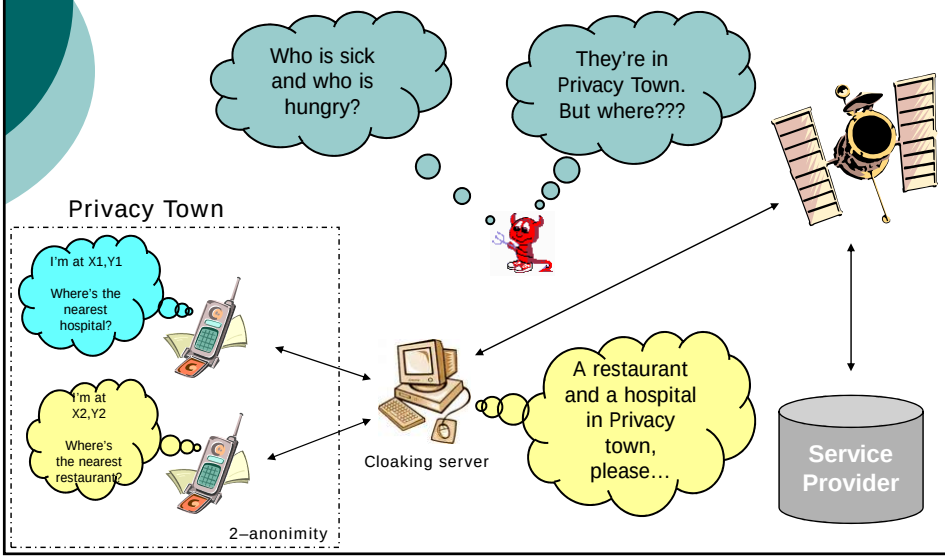
Spatio-Temporal Cloaking

- M. Gruteser and D. Grunwald, Mobisys 2003
- Make data bundled/inaccurate to provide (some degree of) privacy
- LBS do not require high-level of accuracy
  - When requesting the closest hospital, it is not necessary to specify one's exact location; the city/district could be sufficient

Spatio-Temporal Cloacking

- A cloaking server collects requests from several users from the same area during the same period and issues a single request to the LBS server (mixing)
- Size of area and duration of period can be adjusted to increase privacy level

Example of Spatial Cloacking



Cloaking Trade Offs

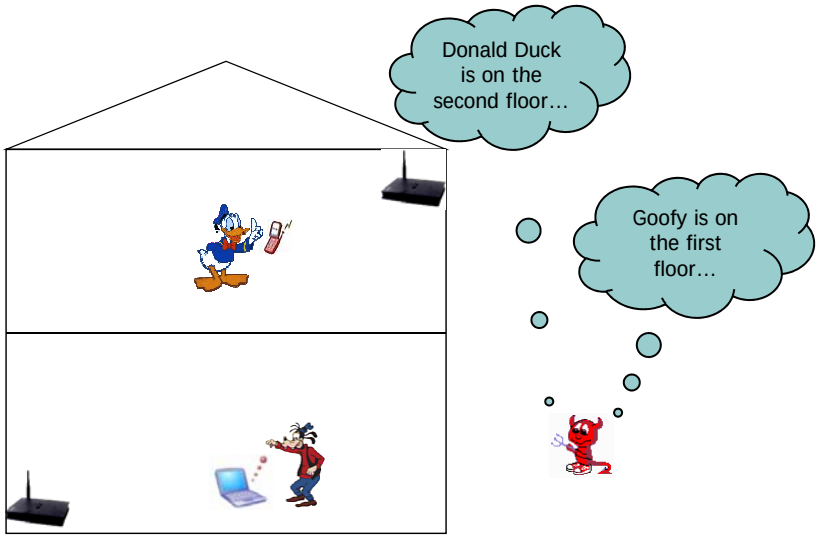
Privacy:

Adversary cannot link any message to any of the k users in the anonymity set

QoS:

Replies might not be accurate and/or timely

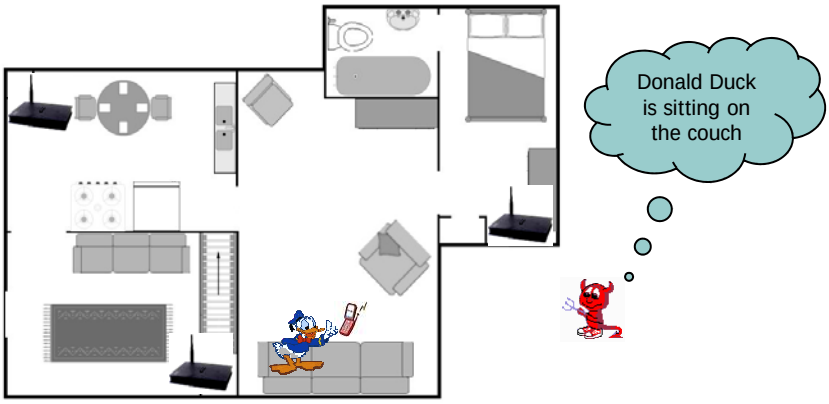
WLAN with multiple access points



WLAN with multiple access points and RADAR

An RF (Radio Frequency) based in building user location and tracking system

Uses empirical signal strength information from multiple access points

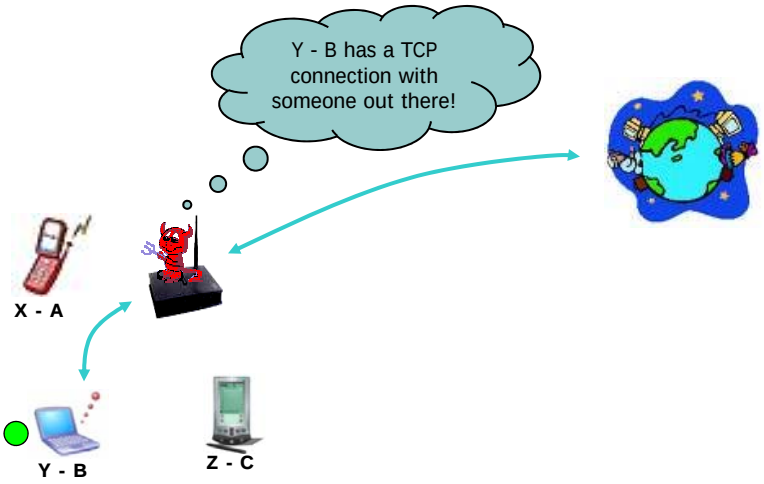


Disposable Interface Identifiers

M. Gruteser and D. Grunwald, WMASH'03

- At each re-association, user randomly chooses a new identifier
- Users can only be tracked for the duration of one session
- Requires re-association and re-establishment of TCP connections
- Involves a random length "silent period" between associations to improve privacy

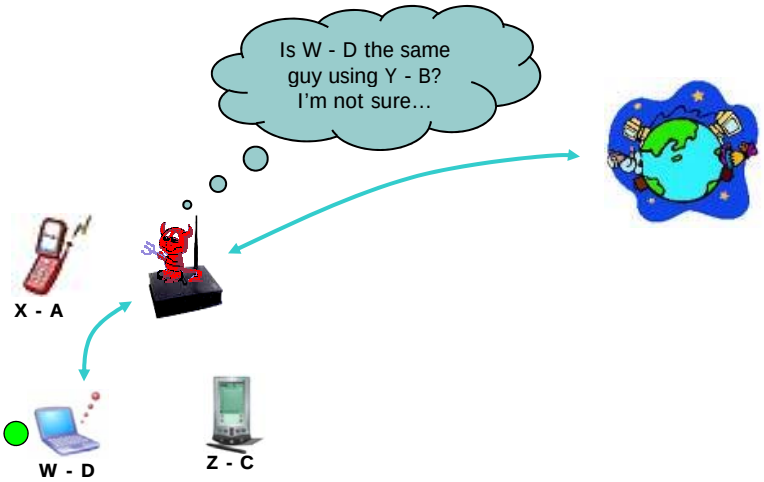
Disposable Interface Identifiers Example



Disposable Interface Identifiers Example

To change its address, the laptop:
- o Turns off its ongoing TCP connections
- o Randomly picks new MAC and IP addresses
- o Re-associates
- o Re-establishs its TCP connections

Disposable Interface Identifiers Example

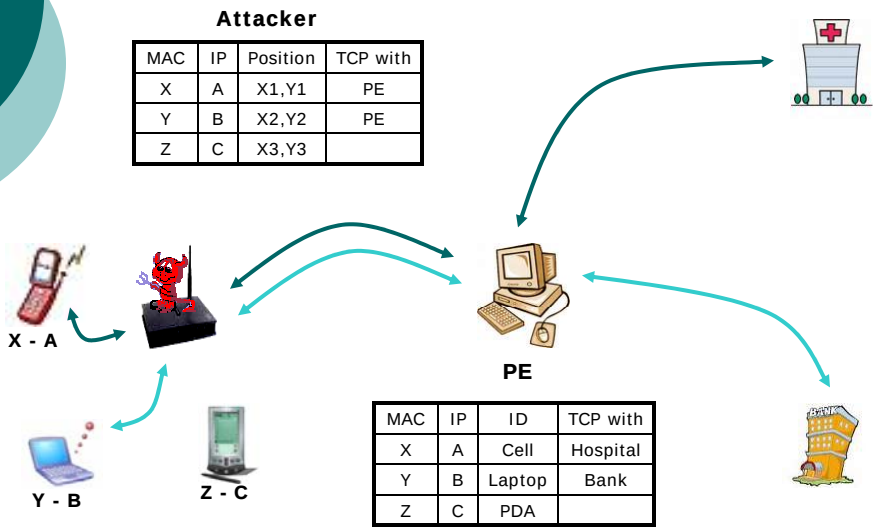


Provacy Enhancement by User Cooperation: PEUC-Win

K. El Defrawy and C. Soriente, NPSec'06

- Users cooperate by exchanging their identifiers periodically
- Requires coordination by server (Privacy Enhancer) external to hosting WLAN
- Does not require re-association or TCP connection re-establishment

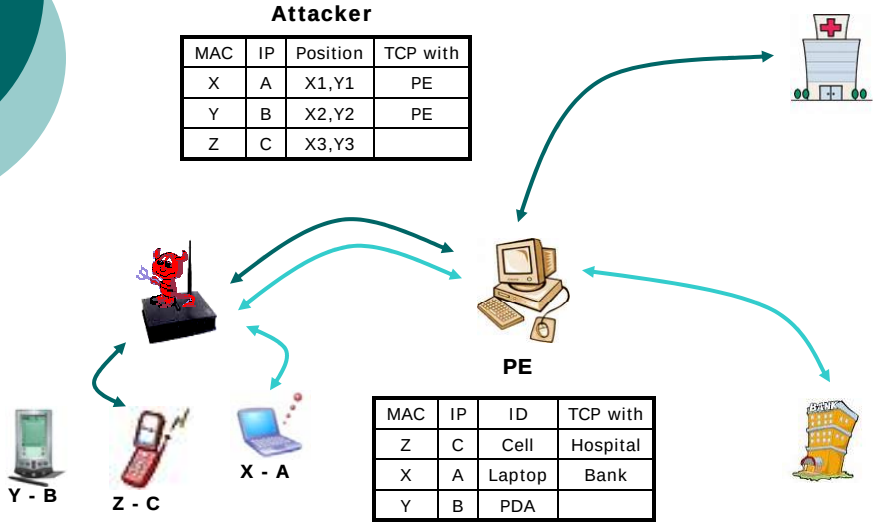
PEUC-Win Example 1



PEUC-Win Example 2

Attacker

MAC	IP	Position	TCP with
X	A	X1,Y1	PE
Y	B	X2,Y2	PE
Z	C	X3,Y3	

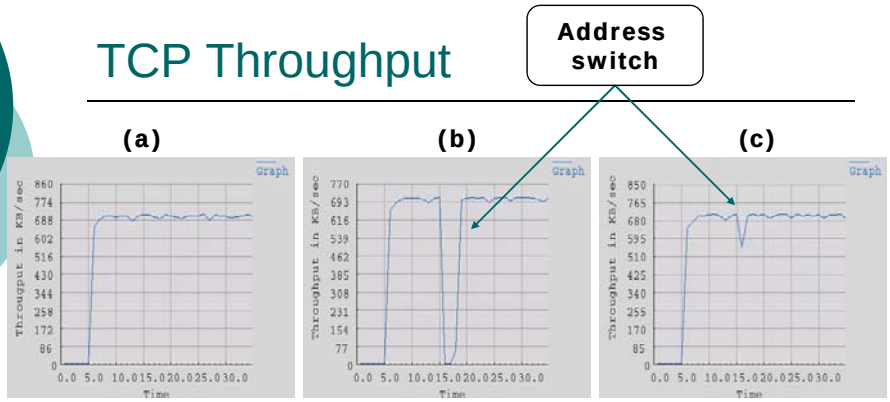


MAC	IP	ID	TCP with
Z	C	Cell	Hospital
X	A	Laptop	Bank
Y	B	PDA	

PEUC-Win – Privacy Enhancer

- ID hopping sequence and time are computed using a hash function and a common seed
- PE provide all information to new group members (pool of IDs, keys, etc.)
  - The pool include pairs of layer2 and layer3 IDs.
  - At the beginning of every period, each peer switches to a new [layer2, layer3]ID-pair.
- PE acts as proxy for all TCP connections
  - All information above layer 3 encrypted
- No TCP connection tear-down ⇨ Higher Throughput!!!
  - But, adapters may need to be shut down to change MAC addresses

TCP Throughput



Average throughput of a TCP connection with:

- no privacy mechanism (a)
- Gruteser method (b)
- PEUC-Win (c)

Challenges and directions

- Take advantage of location and context aware computing, maintaining users' privacy
  - Mechanisms at different levels of the network protocol stack
  - Government / Industry regulations
- Protect users' privacy while maintaining security
  - Total anonymity may lead to security issues
  - In some cases, authorized personnel (system administrators?) must know who is where when

References

- M. Gruteser and D. Grunwald, Anonymous usage of location-based services through spatial and temporal cloaking}, Proceedings of ACM MobiSys, 2003.
- M. Gruteser and D. Grunwald, Enhancing location privacy in wireless lan through disposable interface identifiers: a quantitative analysis, Proc. of 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots, 2003.
- R.P. Minch, Privacy Issues in Location-Aware Mobile Devices, Proceedings of 37th Hawaii International Conference on System Sciences, 2004.
- M. Gruteser and D. Grunwald, A methodological assessment of location privacy risks in wireless hotspot networks, Security in Pervasive Computing, 2004.
- L. Huang, et al., “Silent Cascade: Enhancing Location Privacy Without Communication QoS Degradation”, Security in Pervasive Computing, 2006.
- K. El Defrawy and C. Soriente, PEUC-WiN: Privacy Enhancement by User Cooperation in Wireless Networks, IEEE NPSec06.