Privacy Enhancing Technologies

Carmela Troncoso, KU Leuven (COSIC)

Computer Security Course, University of Vigo

24th-July-2009

Acknowledgements: Dr. Claudia Diaz, Dr. George Danezis

Outline

- Motivation
- What is privacy?
- Anonymous Credentials
- Anonymous communications
- Location Privacy
- Measuring privacy
- Conclusions

Popular arguments against privacy: “You are hiding something”

- “If you care so much about your privacy it’s because you have *something to hide*”
- Solove: “the problem with the ‘nothing to hide’ argument is its underlying assumption that **privacy is about hiding bad things.**”

Popular arguments against privacy: Surveillance = Security?

- Law enforcement keywords to justify more surveillance:
  - Terrorism
  - Child pornography
  - Money laundering
  - Crime

- Public opinion pressure on politicians fuelled by high-impact crimes
  - Making legislation as a response to concrete cases

Problems with surveillance

- Strategic adversaries (e.g., terrorists) adapt while normal citizens don't!
  - Surveillance systems can be evaded
    - Adapting behavioral patterns to remain undetected (financial transactions, mobile phone usage, etc.)
    - Vicious circle: all we need is *more surveillance!*
  - Surveillance facilities may be actually used for crime/terrorism
    - Example: Greek Vodafone scandal: "someone" used the **legal interception functionalities (backdoors) to monitor**: Greek PM, ministers, senior military, diplomats, journalists... (106 people) during the Summer Olympic games of 2004
  - Functionality creep: where do we stop?
    - Once the capability is in place, why not use it to do *more?*

Taking Privacy To Create Security

PRIVACY
SECURITY
THE CHRISTIAN SCIENCE MONITOR
Bennett

Source: http://www.myconfinedspace.com/

Popular arguments against privacy: People don’t care about privacy?

- In the physical world, people are keen on controlling information related to them
  - Who they tell what
    - You might be willing to tell your best friend that you had an argument with your espouse, but you don’t want everybody to know about it
  - Concerns over information taken out of context
    - A picture taken at a crazy party being available to a potential employer
  - We value friends who are discreet and keep our secrets
    - We give more information to people we trust

  - Personal safety
    - Valuable items in an empty house
    - Child alone at home
    - Vulnerability to manipulation
      - □ Smart supermarket that makes you spend more

and what do you care about?

- Would you be happy to broadcast...
  - **Identity attributes:** name, age, gender, race, IQ, marital status, place of birth, address, phone number, ID number...
  - **Location** where you are at a certain point in time, movement patterns
  - **Interests / preferences**: books you read, music you listen, films you like, sports you practice, political affiliation, religious beliefs, sexual orientation
  - **Behavior**: personality type, what you eat, what you shop, how you behave and interact with others
  - **Health data**: medical issues, treatments you follow, DNA, health risk factors
  - **Social network**: who your friends are, who you meet when, your different social circles
  - **Financial data**: how much you earn, how you spend your money, credit card number, bank account

Privacy **is** a security property

- Individuals
  - Freedom from intrusion, profiling and manipulation, protection against crime / identity theft, flexibility to access and use content and services, control over one's information
- Companies
  - Protection of trade secrets, business strategy, internal operations, access to patents
- Governments / Military
  - Protection of national secrets, confidentiality of law enforcement investigations, diplomatic activities, political negotiations
- Shared infrastructure
  - Despite varying capabilities infrastructure is shared
  - Telecommunications, operating systems, search engines, on-line shops, software
  - Denying security to some, means denying it to all!

What is privacy?

What is privacy?

- Abstract and subjective concept, hard to define

- Dependent on cultural issues

- Popular definitions:
  - “The right to be let alone”
    - Focus on freedom from intrusion
  - “Informational self-determination”
    - Focus on control

Regulations

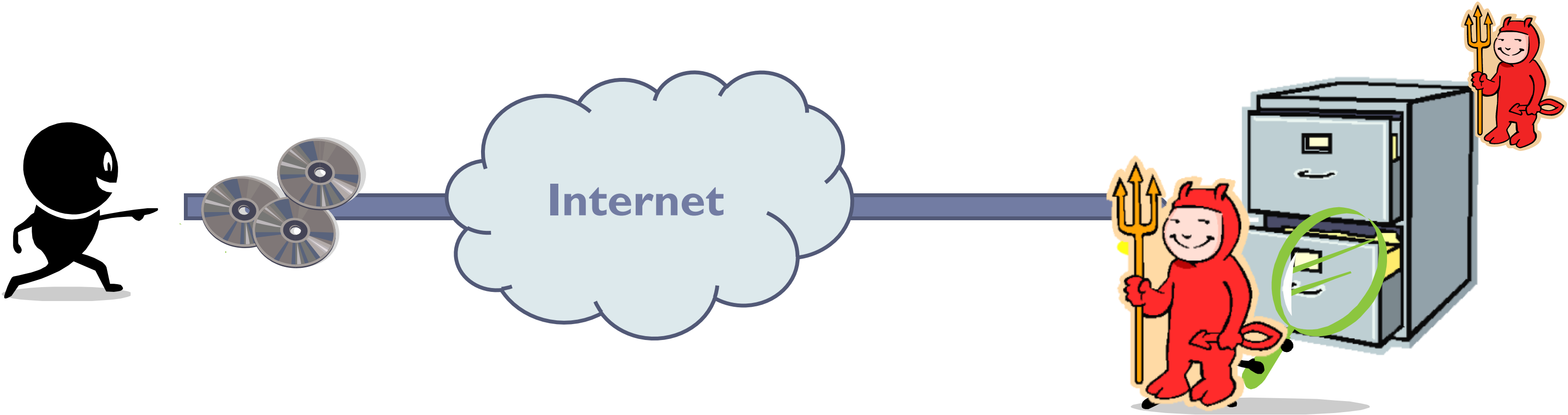
- Data Protection Directive (Directive 95/46/EC)
  - Data collected for a specific and legitimate purpose
  - Data collected must be adequate, relevant and not excessive
    - Principle of proportionality and data minimization
  - With the subject's awareness and **consent** unless...
  - The data subject has the right to access, correct, delete her data
  - Data security
    - Integrity, confidentiality of the data

- Weak enforcement, low penalties
  - Improving a little bit...

Soft Privacy

- Help data controllers manage private information
- "Trusted" party acts as *Controller*
  - Data subject provides data
  - Data controller ensures privacy
    - Policies, access control, right to correct information

- **Threats**: 3rd parties, corrupt insider in honest service provider, errors



Soft Privacy

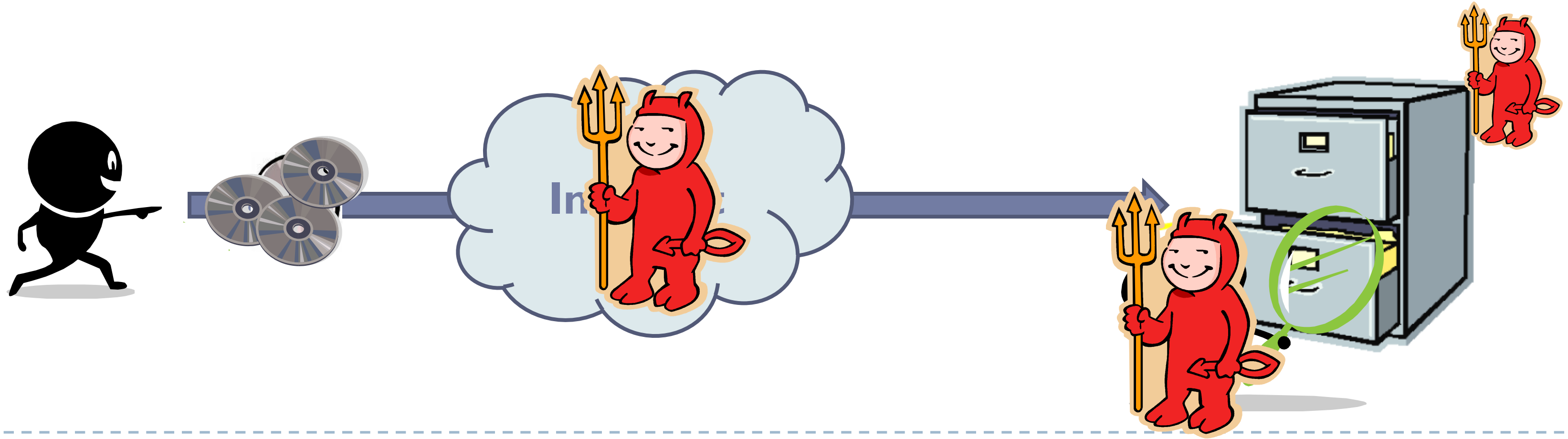
- Data protection principles apply!
  - Limitations on use
  - Limitation on storage time
  - Need for secure storage and access
  - Subject rights
- Mixture of technology, law and enforcement
  - P3P – intent but no enforcement
  - EPAL – IBM enterprise privacy language
- But if it fails… user has already lost control of her data:
  - Millions of exposed records per year due to data breaches at businesses, government agencies and other institutions

Hard Privacy

- Minimize the disclosed information
  - Data Protection data minimization principle

- The data subject is the active security mechanisms user

- **Threats**: communication provider, data holder
  - Minimize the trust in other entities



Privacy properties: **Anonymity**

- Hiding link between identity and action / piece of information.
  - Reader of a web page, person accessing a service
  - Sender of an email, writer of a text
  - Person to whom an entry in a database relates
  - Person present in a physical location

- Pfitzmann-Hansen terminology:
  - *"Anonymity is the state of being not identifiable within a set of subjects, the* anonymity set"
  - "The *anonymity set is the set of all possible subjects who might cause an* action"

- Probabilistic definition

Privacy properties: **Unlinkability**

- Hiding link between two or more actions/identities/info pieces
  - Two anonymous letters written by the same person
  - Two web page visits by the same user
  - Entries in two databases related to the same person
  - Two people related by a friendship link
  - Same person spotted in two locations at different points in time

- Pfitzmann-Hansen terminology:
  - *"Unlinkability of two or more items means that within a system,* these items are no more and no less related than they are related concerning the a-priori knowledge"

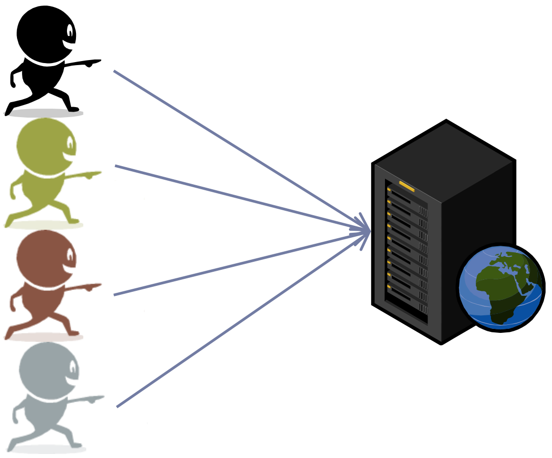
Privacy properties: **Unobservability**

- Hiding user activity.
  - Impossible to see whether someone is accessing a web page
  - Impossible to know whether an entry in a database corresponds to a real person
  - Impossible to distinguish whether someone or no one is in a given location

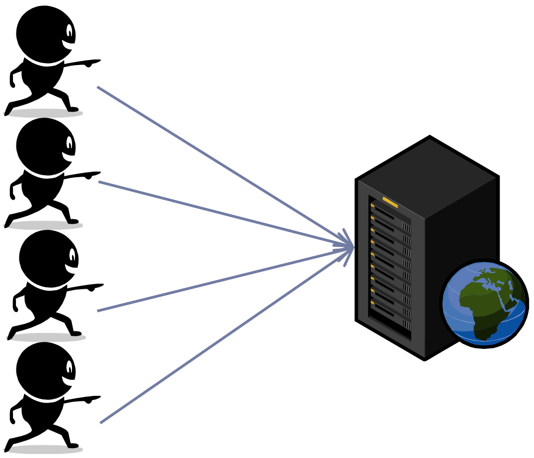
- Pfitzmann-Hansen terminology:
  - *"Unobservability is the state of items of interest being* indistinguishable from any item of interest at all"
  - *"Sender unobservability then means that it is not noticeable* whether any sender within the unobservability set sends."

Privacy properties: **Pseudonymity**

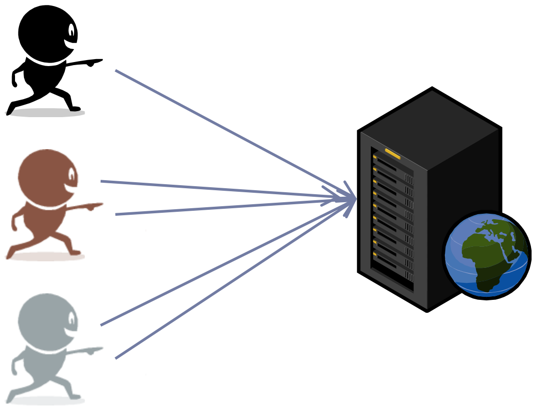
- Pfitzmann-Hansen terminology:
  - *“Pseudonymity is the use of pseudonyms as IDs.”*
  - “A *digital pseudonym is a bit string which is unique as ID and which can* be used to authenticate the holder”



One time pseudonyms (Anonymity)



Persistent pseudonyms (Identity!)



Hybrid (Multiple identities)

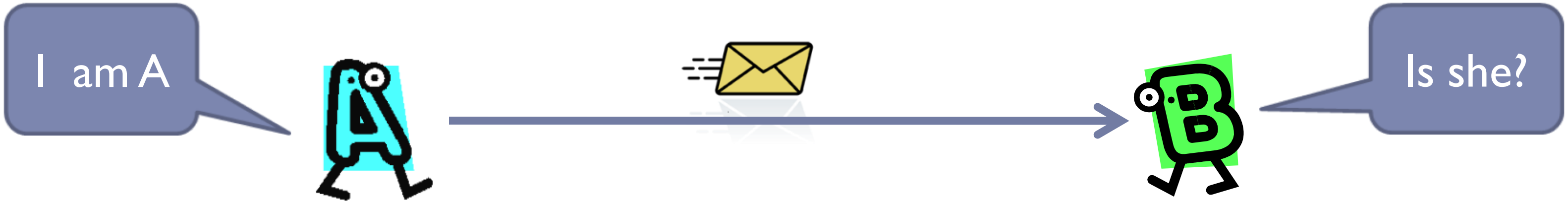
Privacy properties: **Plausible deniability**

- Not possible to prove user knows, has done or has said something
  - Off-the-record conversations
  - Resistance to coercion:
    - Not possible to prove that a person has hidden information in a computer
    - Not possible to know that someone has the combination of a safe
  - Possibility to deny having been in a place at a certain point in time
  - Possibility to deny that a database record belongs to a person

Anonymous credentials

Again, we speak about authentication

- First step before any security policy can be applied



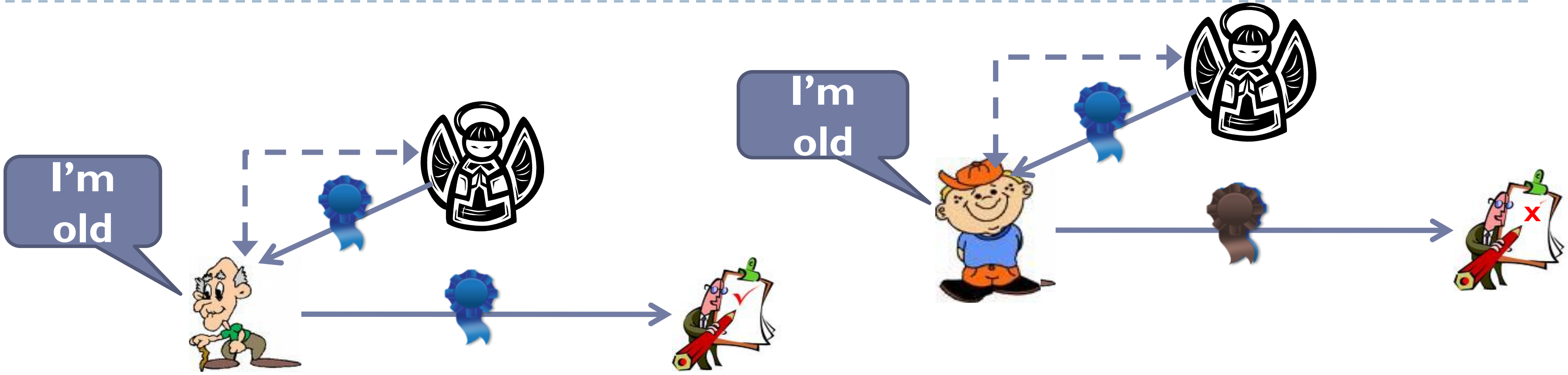
- Makes sense in government, military, even commercial
  - ...but if there is no closed group? (e.g., peer-to-peer)
  - The **Identity Management** concept

- Possible solutions:
  - Private authentication: hide against 3rd parties
  - Anonymous credentials: protect against everybody

Idea behind credentials

- Many transactions involve attribute certificates
  - ID docs: state certifies name, birth dates, address
  - Letter reference: employer certifies salary
  - Club membership: club certifies some status
  - PKI certificate: RRN in Belgian eID (couldn't find Spanish...)
- Do you want to show all of them?
- Credential: token certifying one attribute
  - e.g. going to the cinema
  - Digital credentials: string, boolean attributes, range

Properties



- **Completeness**: if the statement is true, the verifier will be convinced
- **Zero-knowledge**: if the statement is true no cheating verifier learns anything other than this fact
- **Soundness**: no cheating prover can convince the honest verifier

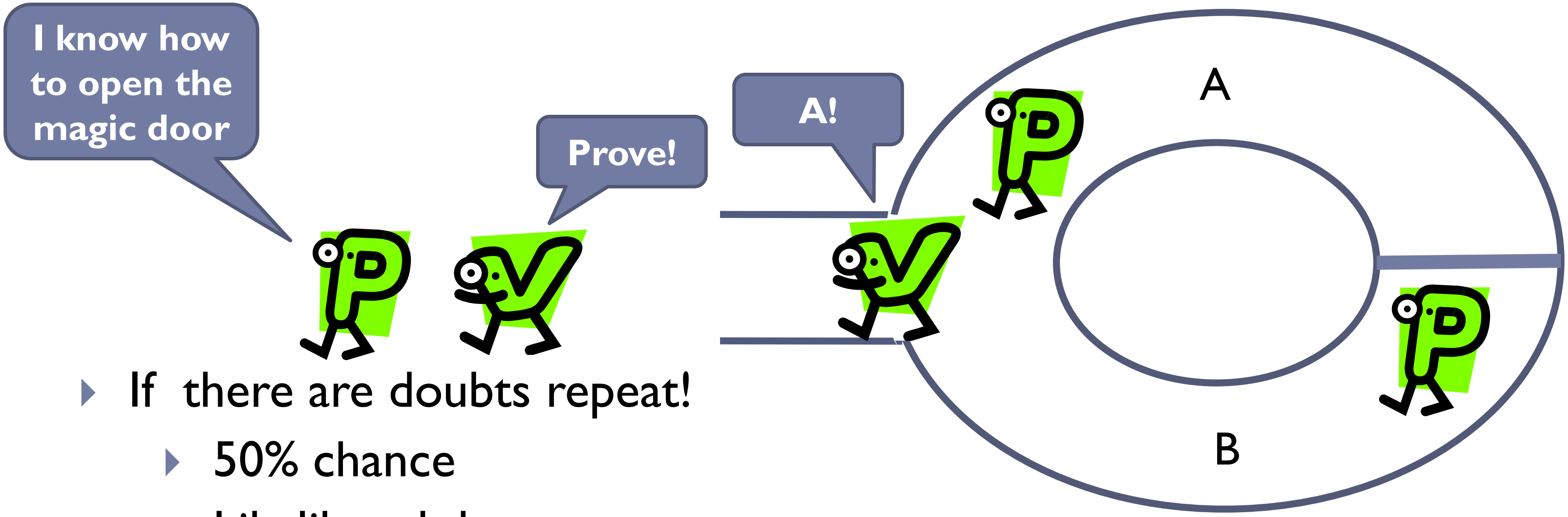
- **Unlinkability**: two requests cannot be liked to the same user

- Holds even if verifier and prover collide

Zero-knowledge proofs

- One party to prove to another that a statement is true, without revealing anything other than the veracity of the statement.

- J.J. Quisquater: "How to Explain Zero-Knowledge Protocols to Your Children"



- If there are doubts repeat!
  - 50% chance
  - Likelihood decreases

PKI vs Anonymous Credentials

PKI

Signed by a trusted issuer

Certification of attributes

Authentication (secret key)

Double-signing detection

No data minimization

Users are identifiable

Users can be tracked
(Signature linkable to other contexts where PK is used)

Anonymous credentials

Signed by a trusted issuer

Certification of attributes

Authentication (secret key)

Double-signing detection

Data minimization

Users are anonymous

Users are unlinkable in different contexts

Types of credentials

- Original idea Chaum
  - Needed 3rd Party to produce new pseudonyms

- Brands-Credentials:
  - One-show
  - Credentica – uProve (Microsoft, Card Space)

- CL-Credentials (Camenish Lysyanskaya)
  - Multi-show (detect misbehaviour)
  - Less efficient
  - Idemix (IBM) - Free source? ... the patents war

Applications

- Anonymous authentication
  - *Privacy Preserving Electronic Petitions*. Claudia Diaz, Eleni Kosta, Hannelore Dekeyser, Markulf Kohlweiss, and Girma Nigusse. In Journal of Identity in the Information Society (IDIS), (in print) 14 pages, 2009
- Anonymous e-cash
  - *Untraceable Electronic Cash*. David Chaum, Amos Fiat and Moni Naor. Crypto'89
- Muti-show credentials
  - *How to Win the Clone Wars: Efficient Periodic n-Times Anonymous Authentication,* by Jan Camenisch, Susan Hohenberger, Markulf Kohlweiss, Anna Lysyanskaya and Mira Meyerovich. ACM CCS 2006.
- Anonymous tokens for reputations systems
  - "Making P2P Accountable without Losing Privacy." Mira Belenkiy, Melissa Chase, C. Chris Erway, John Jannotti, Alptekin Küpçü, Anna Lysyanskaya, Eric Rachlin.

The challenge

- Make them usable in every context!
  - eID, ePassport
  - Any smart card
  - One day RFID??

Anonymous communications

Anonymous communications

- Hidden assumptions
  - Secure channel
  - The channel does not break the privacy property

- But IP is a pseudo-identifier!
  - anonymous credentials are useless in this case...

- Need protection against **traffic analysis**
  - the military also use internet...

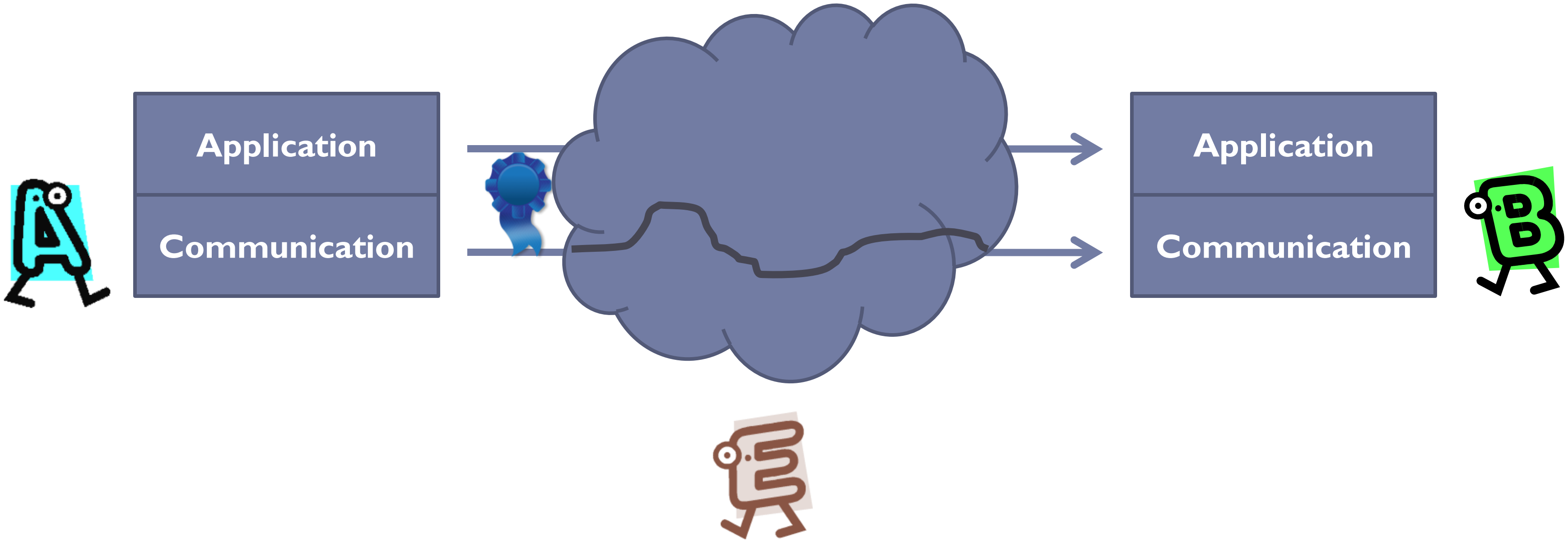
Traffic analysis

- Even if communication is encrypted, traffic data can reveal a lot of information: source, destination, timing, volume, etc.

- Examples from WW II (signals intelligence):
  - Traffic analysis was used by the British at Bletchley Park to assess the size of Germany's air-force
  - Japanese traffic analysis countermeasures contributed to the surprise of their 1941 attack on Pearl Harbour
  - Increased volume: possible imminent action (example: D-day)
  - Identifying people by their typing

- Examples from today
  - Google uses the incidence of links to assess the relative importance of web pages
  - Credit card companies examine transactions to spot fraudulent patterns of spending

System model



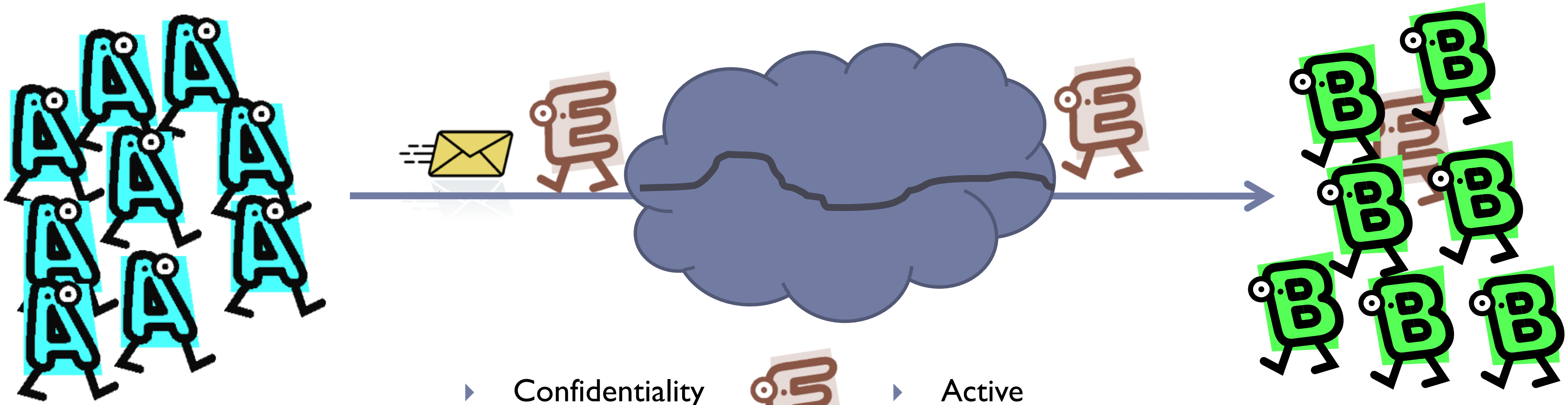
Application

Communication

Application

Communication

Adversarial model



- Confidentiality
- Integrity
- Authentication
- Non repudiation
- Availability

- Active
- Passive

- Global
- Partial

- Internal
- External

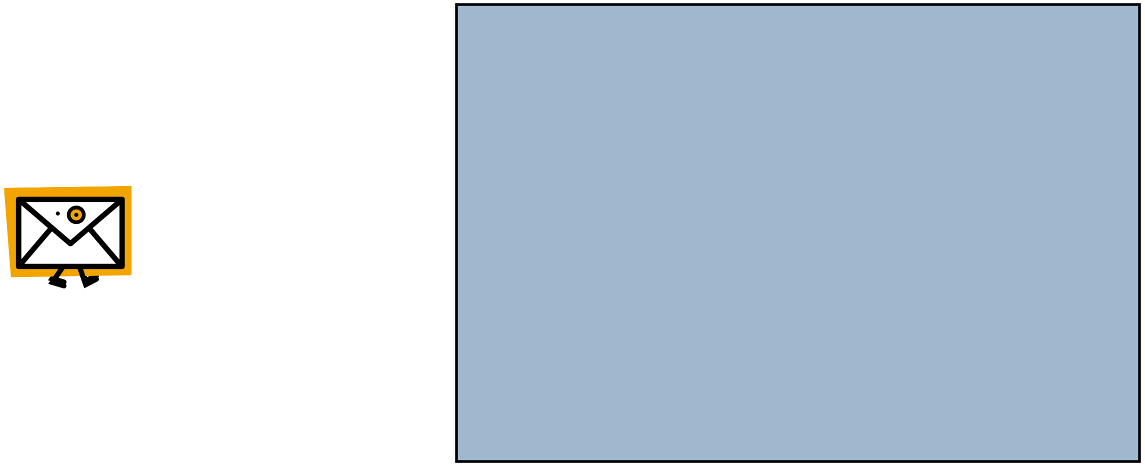
Attacker assumptions

- Attacker abilities:
  - Observe
    - All links (*Global Passive Adversary*)
    - *Some links*
  - Modify, delay, delete or inject messages.
  - Control some nodes in the network.

- Attacker limitations:
  - Cannot break cryptographic primitives.
  - Cannot see inside nodes he does not control.

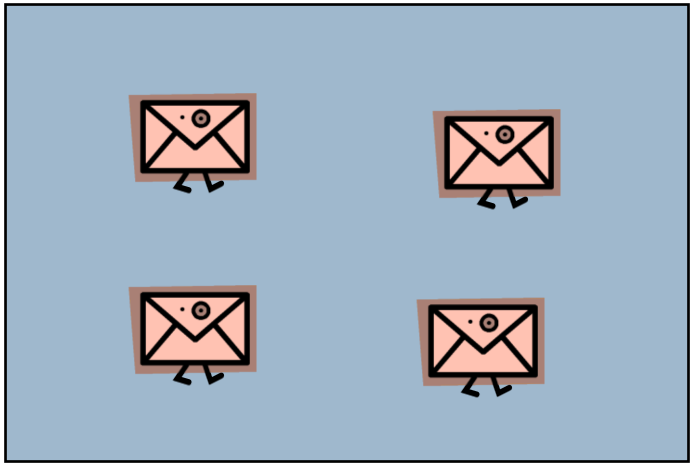
Concept of Mix (Chaum 1982)

Router that hides correspondence between inputs and outputs



Concept of Mix: mix and flush

Router that hides correspondence between inputs and outputs



Functionality of Mixes

- Mixes modify
  - The appearance of messages
    - Encryption / Decryption
      - □ $\text{Sender} \rightarrow \text{Mix}_1 : \{\text{Rec}, \text{msg}\}_{K_{\text{Mix}_1}}$
    - Padding / Compression
    - Substitution of information (e.g., IP)
  - The flow of messages
    - Reordering
    - Delaying - Real-time requirements!
    - Dummy traffic - Cost of traffic!

Pool Mixes

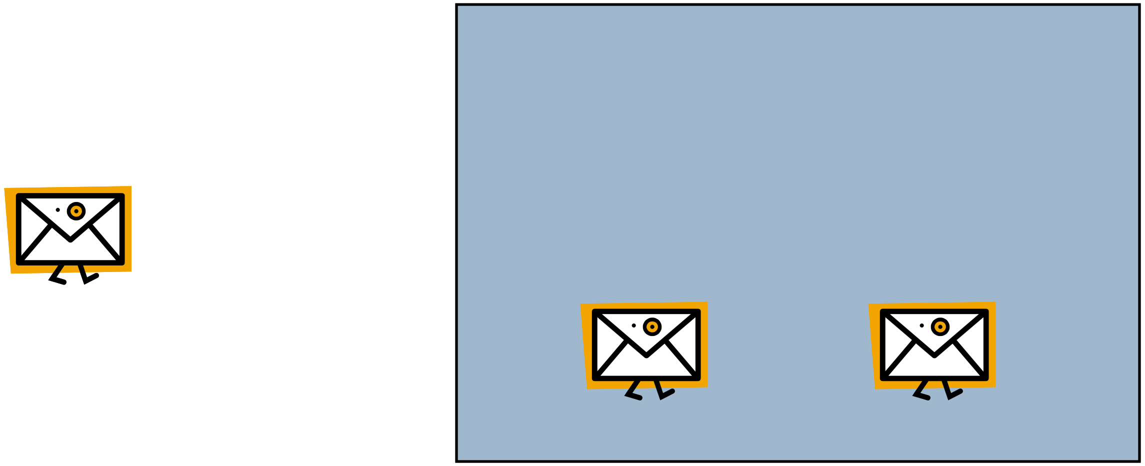
- Based on the mix proposed by Chaum in 1981:
  1. Collect ***N*** inputs
  2. Shuffle
  3. Flush (Forward) ***F*** inputs

  Round
- Pool selection algorithm
  - No pool / Static pool (***F<N***) / Dynamic pool (***F(t)***)
  - Influences the performance and anonymity provided by the mix
- Flushing condition
  - Time / Threshold
  - Deterministic / Random

Example of pool mix

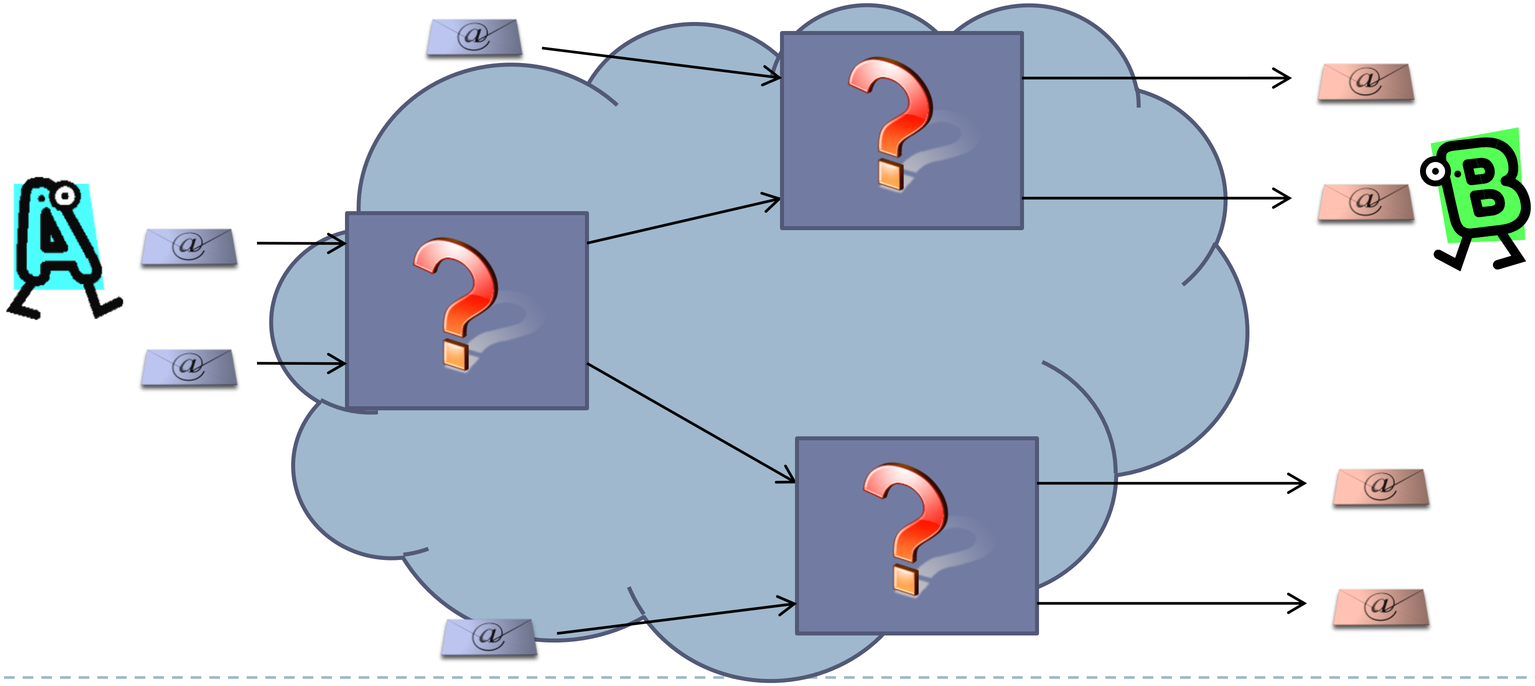
Deterministic threshold
static pool Mix

Pool = 2
Threshold = 4

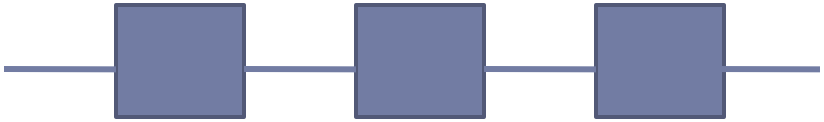


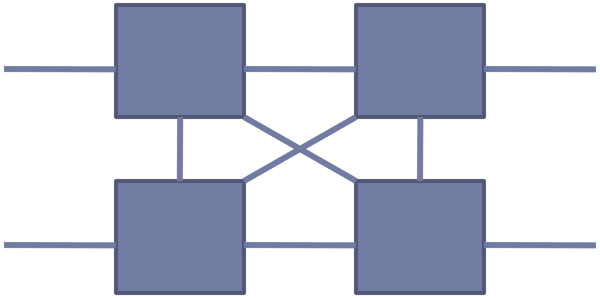
Mix networks

- Mixes are combined in networks in order to
  - Distribute trust (one good mix is enough)
  - Load balancing (no mix is big enough)
  - Alice → (Mix1,{Mix$_2$, {Bob, msg}$_{K_{Mix_2}}$} $_{K_{Mix_1}}$})



Cascades vs Free Route topologies





- Surface of attack
  - Advantage free routes
- Availability
  - Advantage free routes
- Intersection attacks
  - Advantage cascades (anonymity set smaller but no partitioning possible)
- Trust
  - Advantage free routes (more choices available to user)

Peer-to-peer vs client-server architectures

- Surface of attack
  - Advantage peer-to-peer
- Liability issues
  - Advantage client-server
- Resources / incentives / quality of service
  - Advantage client-server
- Availability
  - Advantage peer-to-peer
- Sybil attacks
  - Advantage? Depending on admission controls (for peers/servers)

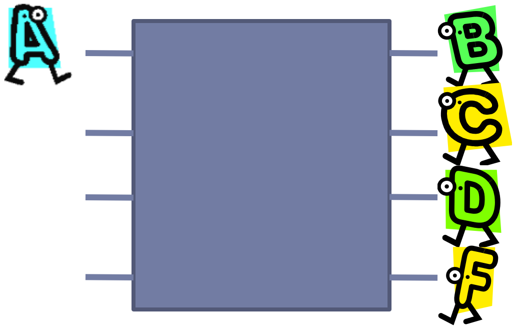
Mix Deployed systems

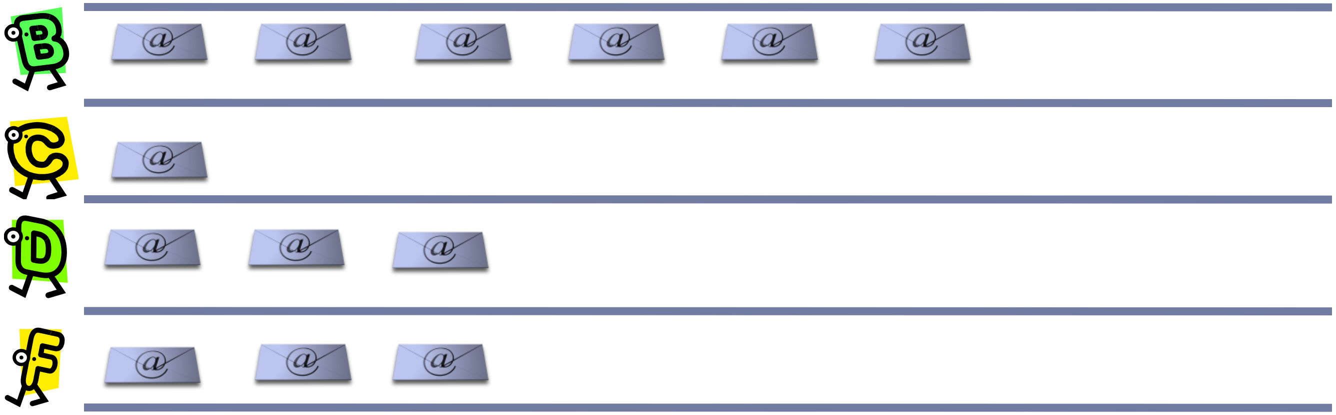
- Mixmaster (Cottrell et al. evolving since 1995)
  - Fixed size (padding / dividing large messages)
  - Integrity protection measures
  - Multiple paths for better reliability
  - No replies
- Mixminion (Danezis et al., 2003)
  - SURBs (Single-Use Reply Blocks)
  - Packet format: detection of tagging attacks (all-or-nothing)
  - Forward security: trail of keys, updated with one-way functions
  - Vulnerabilities found in 2008
- Sphinx (Danezis and Goldberg, 2009)
  - Will it be deployed?
  - Based on Eliptic Curves

Long-term intersection attacks

- Family of attacks with many variants:
  - Disclosure attack (Agrawal, Kesdogan)
  - Hitting set attack (Kesdogan)
  - Statistical disclosure attack (Danezis, Serjantov)
  - Extensions to SDA (Dingledine and Mathewson)
  - Two-Sided SDA (Danezis, Diaz, Troncoso)
  - Perfect-Matching disclosure attack (Troncoso et al.)
- Assumptions:
  - Alice has persistent communication relationships (she communicates repeatedly with her friends)
  - Large population of senders, and a different subset mixes their messages with hers in each round

Long-term intersection attacks





Dummy traffic

- Fake messages/traffic introduced to confuse the attacker
  - Undistinguishable from real traffic

- These messages may be generated
  - By users
  - By mixes

- Dummies improve the anonymity by making more difficult the traffic analysis

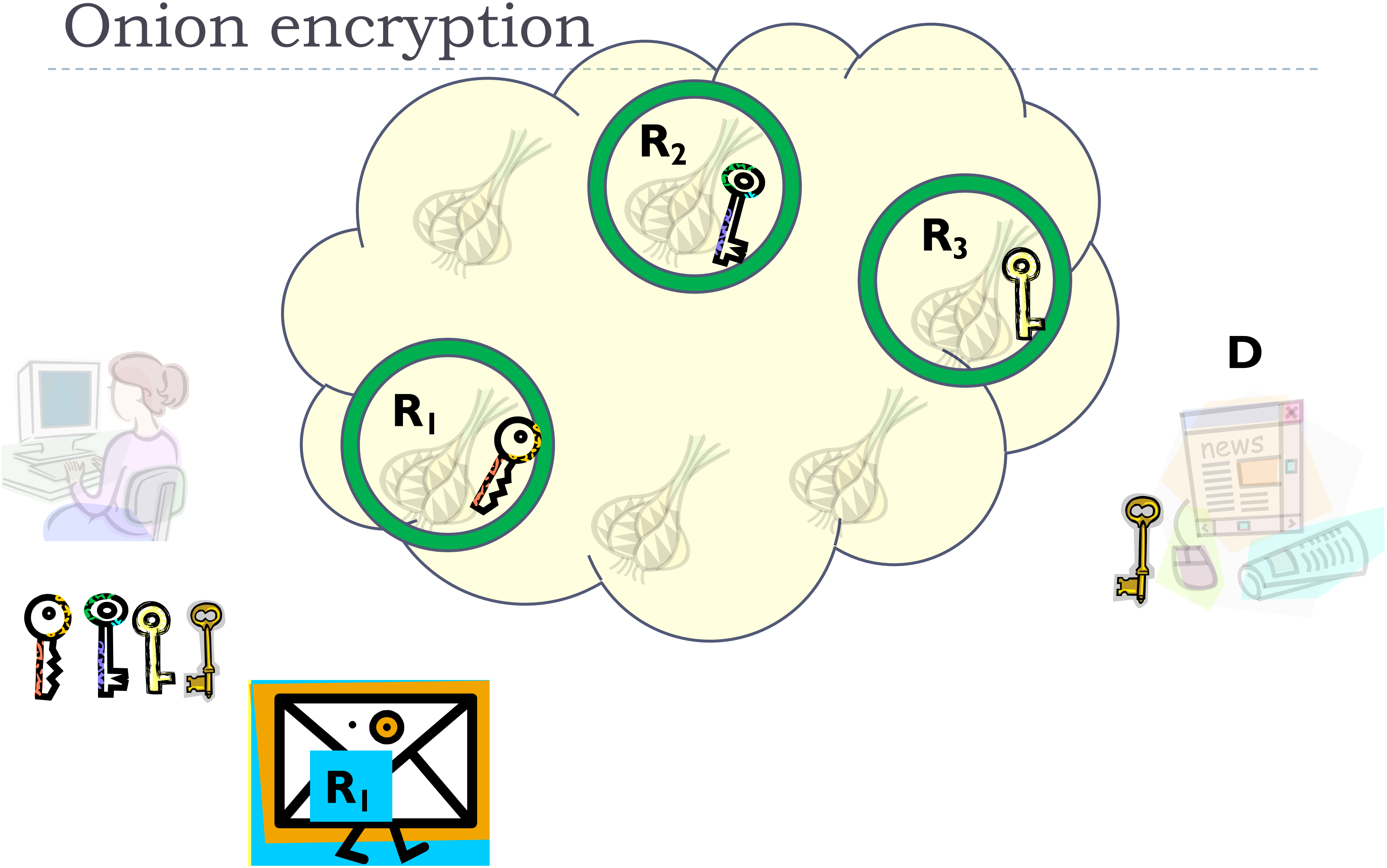
- Neccessary for unobservability

- Dummy traffic is expensive (bandwidth)
  - Unclear how to use it in an optimal way

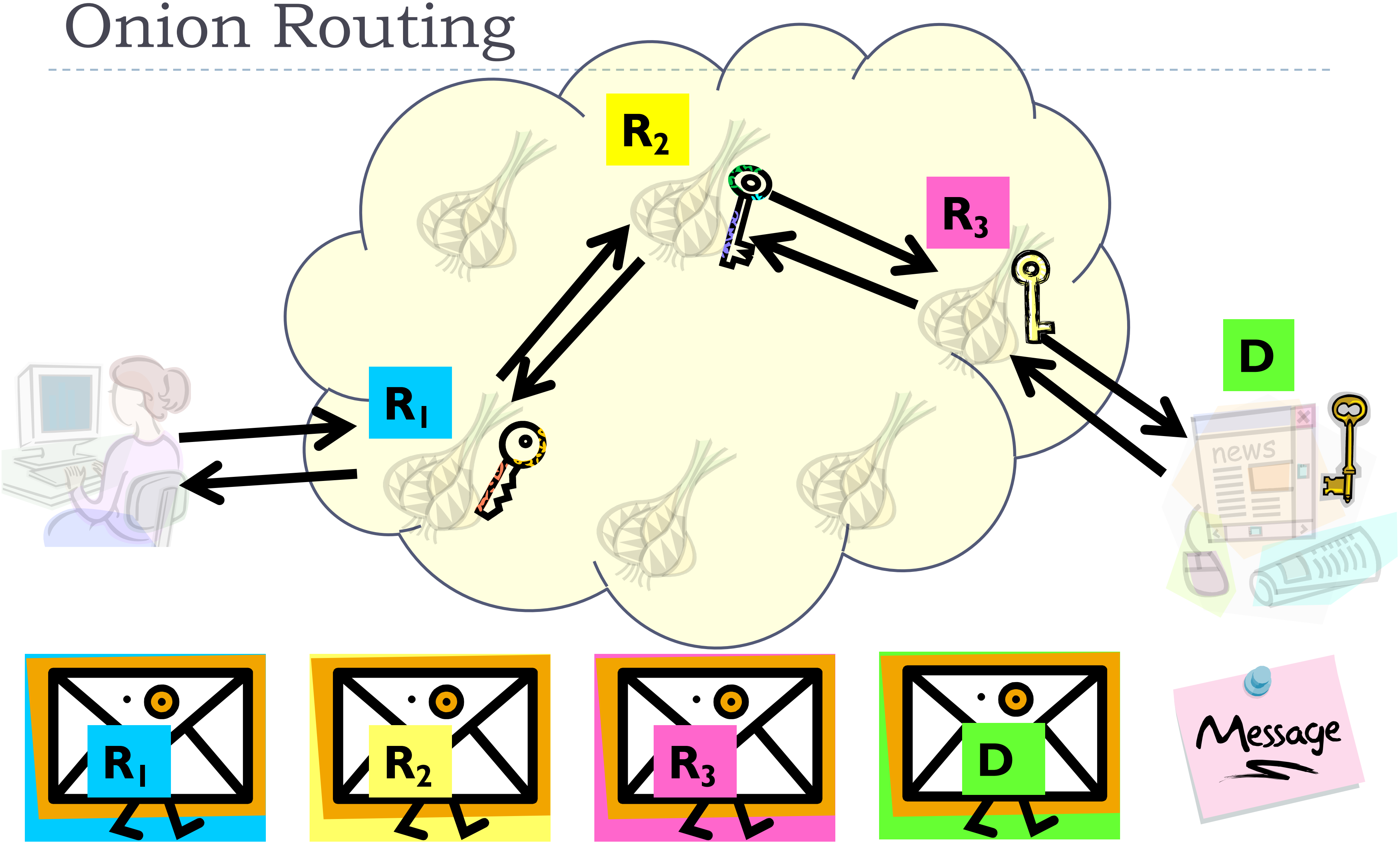
What about web traffic?

- No more collection of messages
  - Needs to be real time!
- Difficult to conceal traffic pattern
  - Difficult to pad
    - Lots of padding: scalability / cost problem
    - Little padding: not enough to conceal pattern
- Vulnerable to strong adversaries (entry+exit)
- Fingerprinting attacks
  - Adversary observes only user side
- Internet exchanges: global adversary

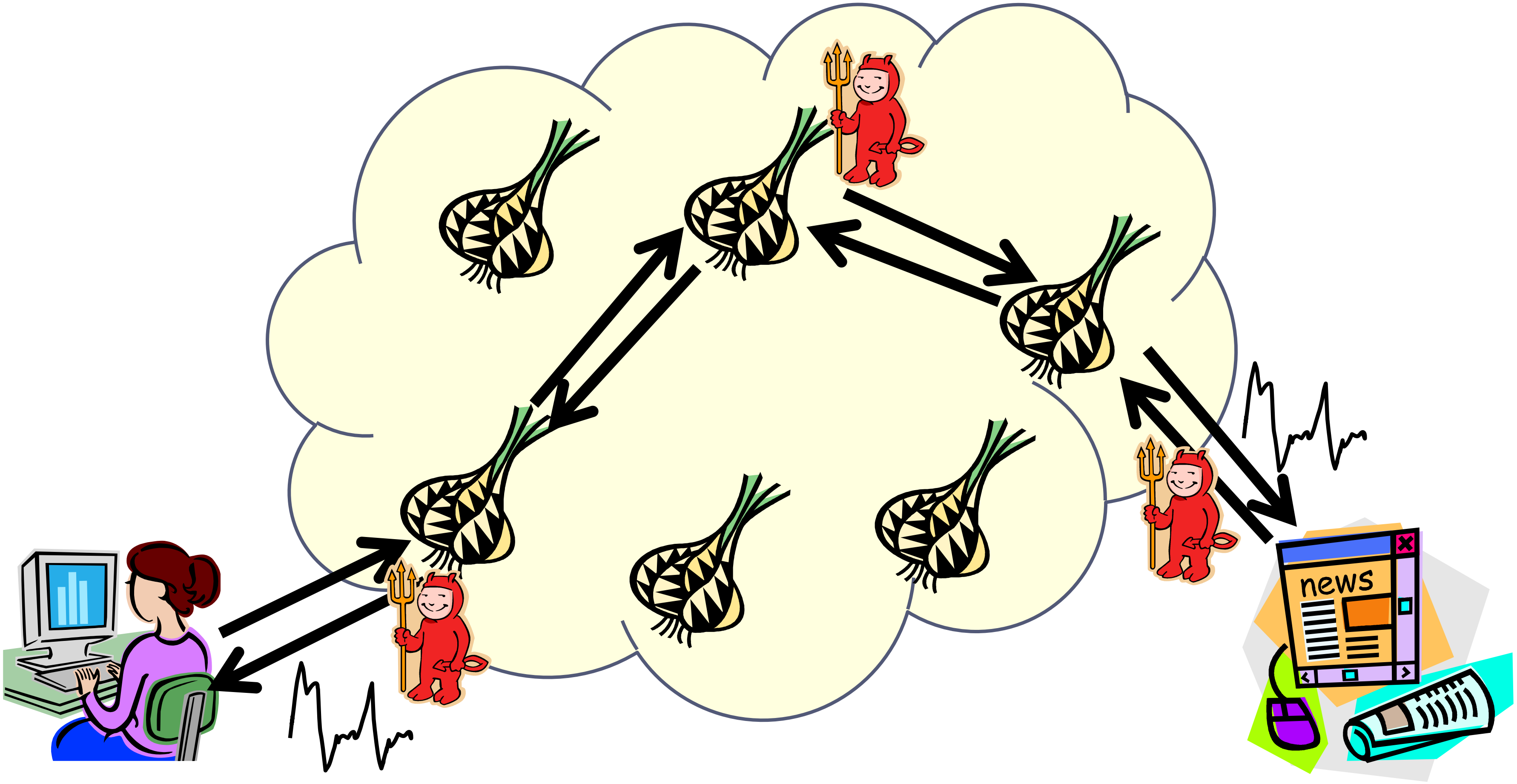
Onion encryption



Onion Routing



TOR – adversary model



Location Privacy

How many ways have you been located today?

- When I carry my cell phone, turned on,
- When I used my laptop computer,
- When I used a credit card at the gas station,
- When I put my card in the ATM machine,
- When I drove through a monitored intersection,
- When I walked by the security camera at the supermarket,
- When I scanned my badge to enter a building,
- When I passed by a Bluetooth-enabled printer…

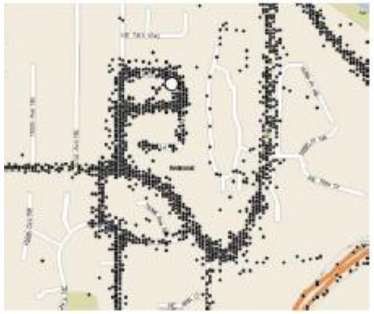
Location Based Services

- Location-based traffic Monitoring and emergency services
  - e-Call, VII, traffic congestion control
- Location finder:
  - Where is the nearest theatre, restaurant, gas station,...
- Variable pricing applications
  - Congestion pricing
  - Pay-as-you-drive
- Social applications
  - Geotagged Twitter
  - Google Latitude

Why is this a problem?

- Do you want to be seen at certain locations?
  - abortion clinic, AIDS clinic, business competitor, or political headquarters. (Google Street View)

- What can be automatically inferred about a person based on location?
  - Any important location…
    - Desk in a building [BeresfordStajano03]
    - Home location [Krumm07, Hoh et al06]
    - Future locations [Krumm06]
  - And even identification!
    - http://www.batchgeocode.com/lookup/

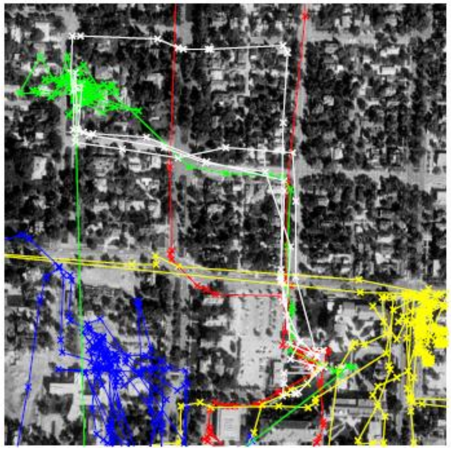


Source: John Krumm, "A survey of computational location privacy", *Personal and Ubiquitous Computing,* Volume 13, Issue 6, 2008

- Let's anonymize!

Does it work?

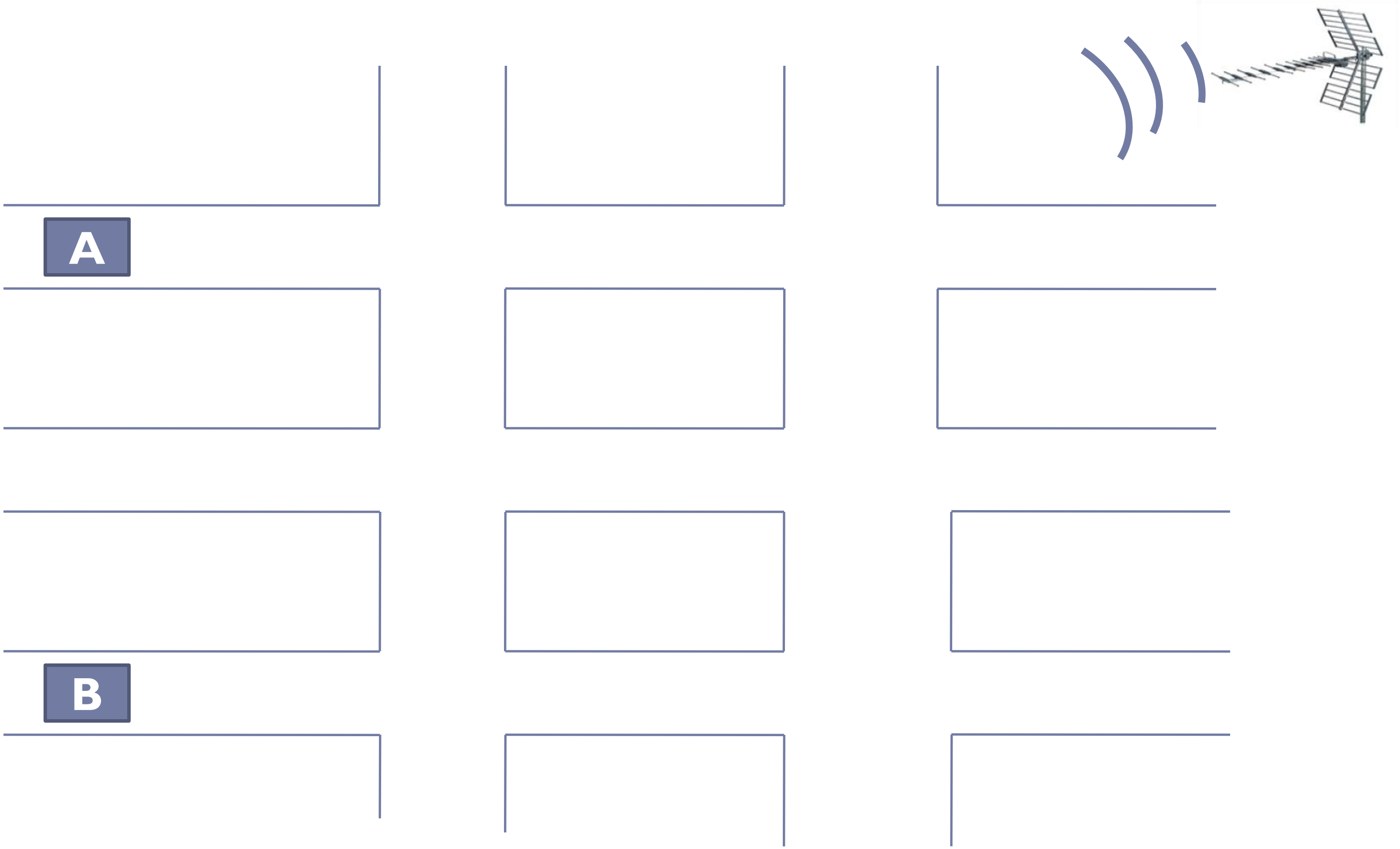
- One pseudonym per sample



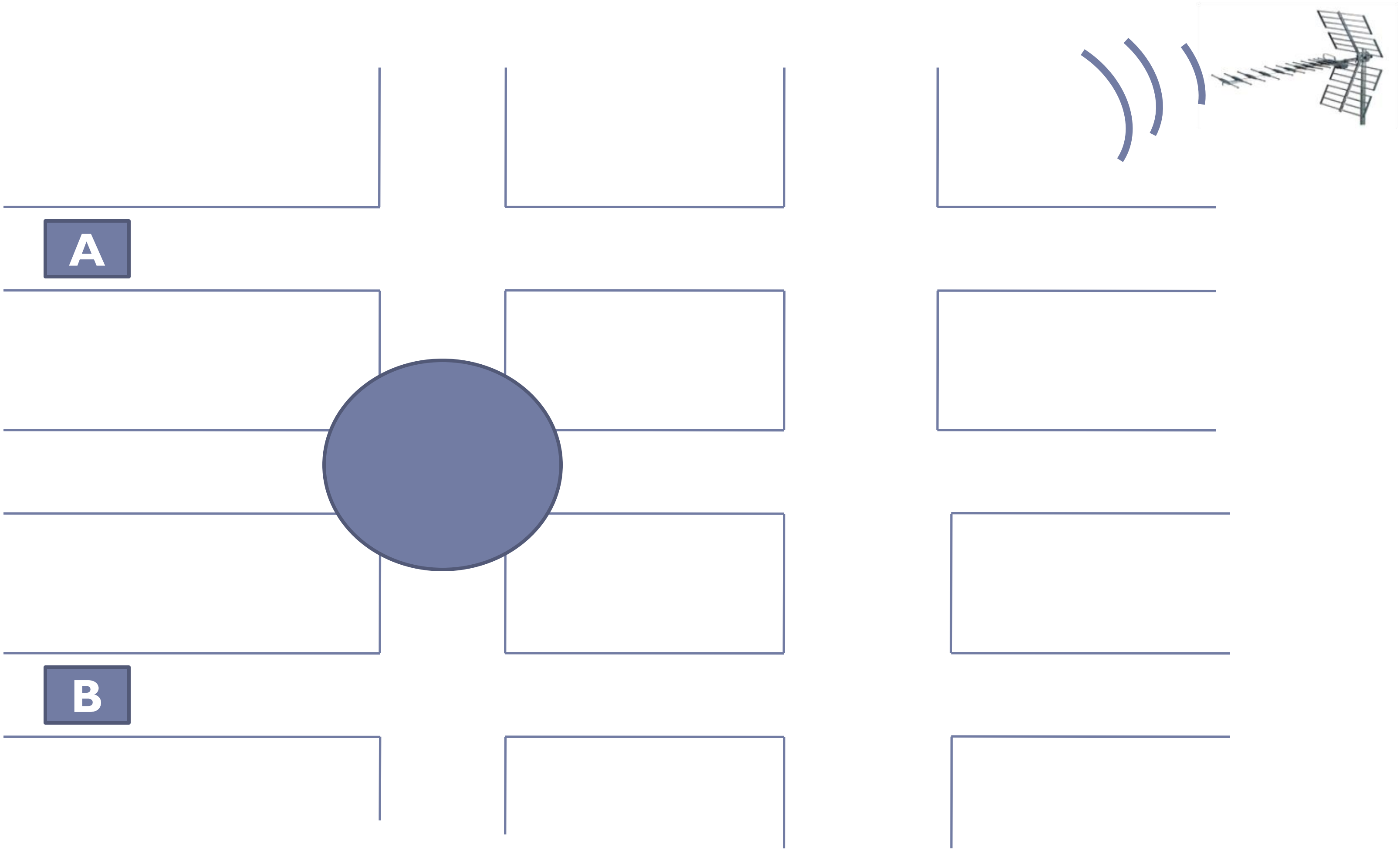
Source: Marco Gruteser, Baik Hoh: On the Anonymity of Periodic Location Samples. SPC 2005:

- Multi-target tracking
  - Only 5 people…
- Why is it so difficult?
  - Real time
  - Space-Time relation
  - Dummy traffic?

Defenses: Mix Zones



Defenses: Mix Zones



Mix zones: limitations

- How is the mixing done?
  - Exchange?
  - Individual pseudonym change
    - Authentication? anonymous credentials are slow…
- Where do we place them?
- What if there are no other cars?

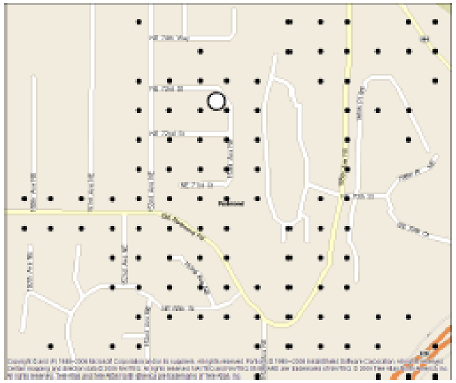
Defenses: Location Perturbation

- Clients do not trust the LBSs with policy-based location privacy protection

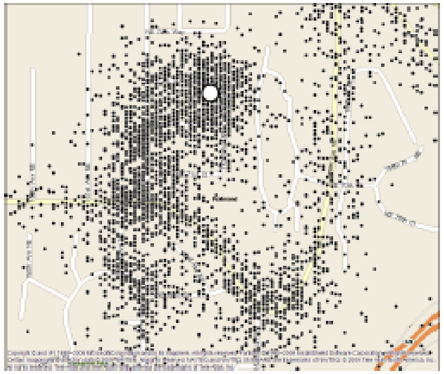
- Main ideas
  - Applications can tolerate *inaccurate location data to a certain* degree
  - Location perturbation provides inability for adversaries to know or infer exact location of a user through location based inference
- Approaches:
  - Simple perturbation
  - Spatial Cloaking
  - Spatio-temporal Cloaking
  - Many more…

Defenses: Simple perturbation

- Discretization [Krumm07]

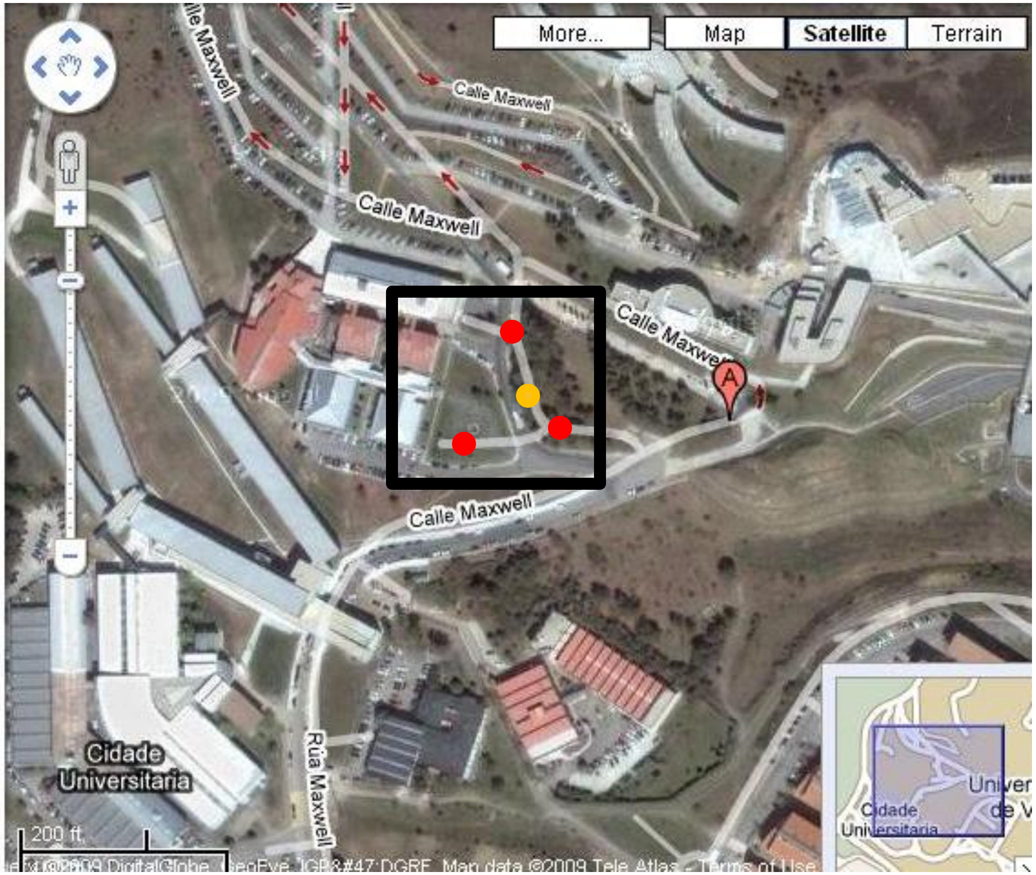


- Additive Noise [Krumm07]



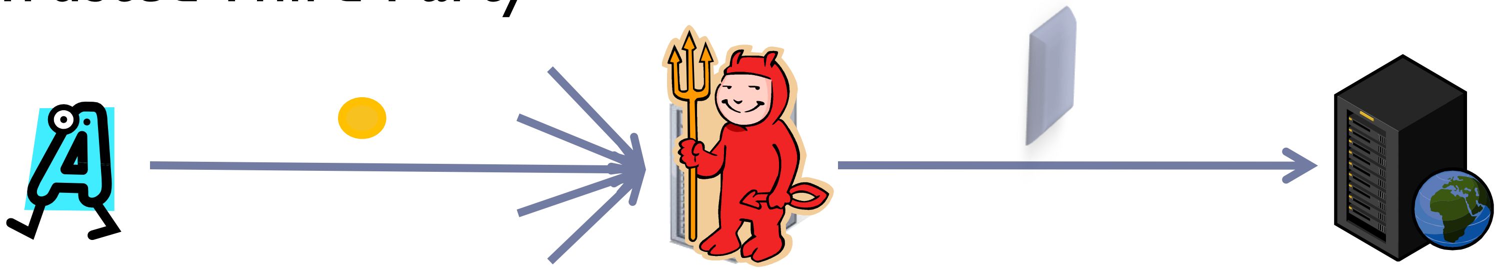
Defenses: Spatial cloaking

- *k*-anonymity:
  - *"A user cannot be distinguished from at least k-1 individuals"* [Sweeney02]
  - Bigger *k*, bigger region
  - ...and if no people around?

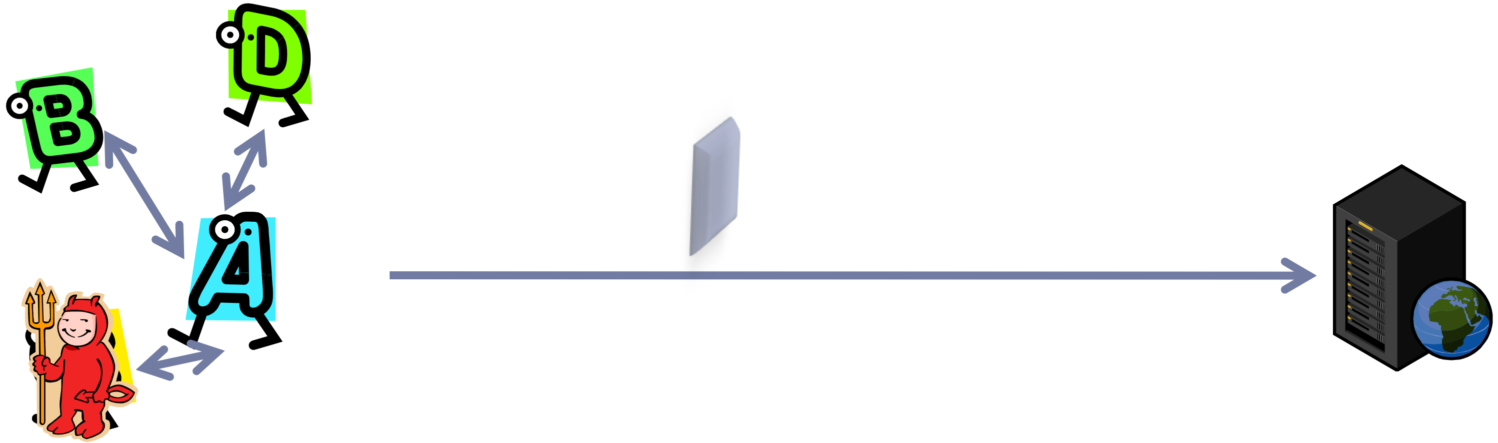


Implementations

- Trusted Third Party

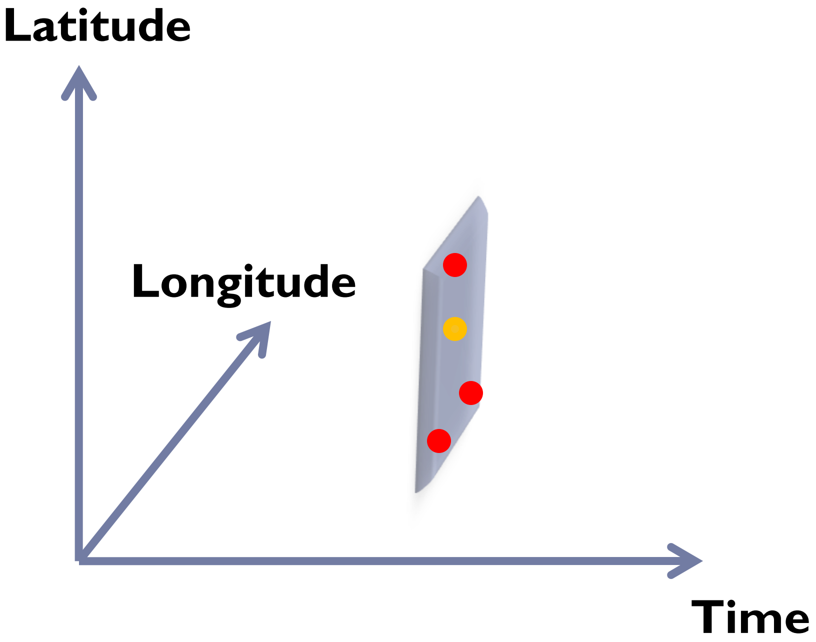


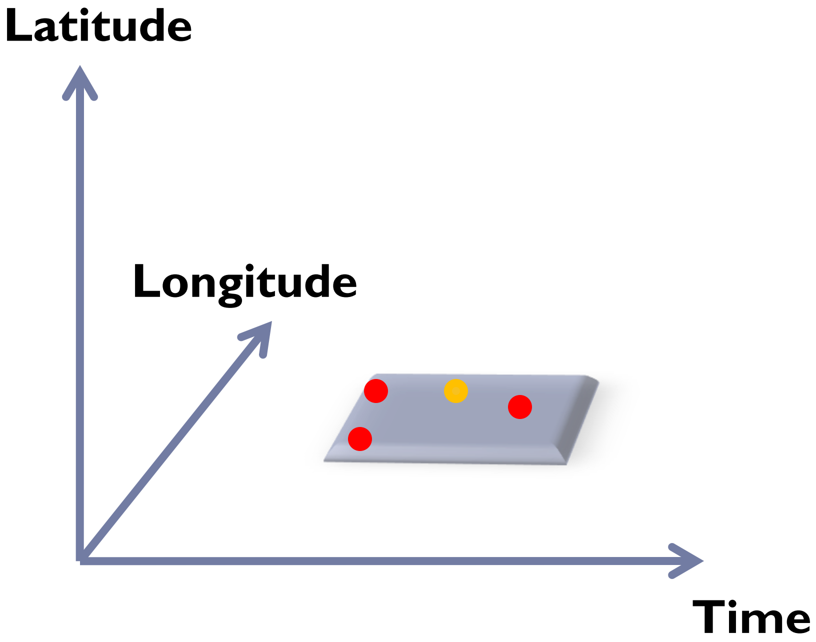
- Collaborative approaches



Defenses: Spatial vs temporal cloaking

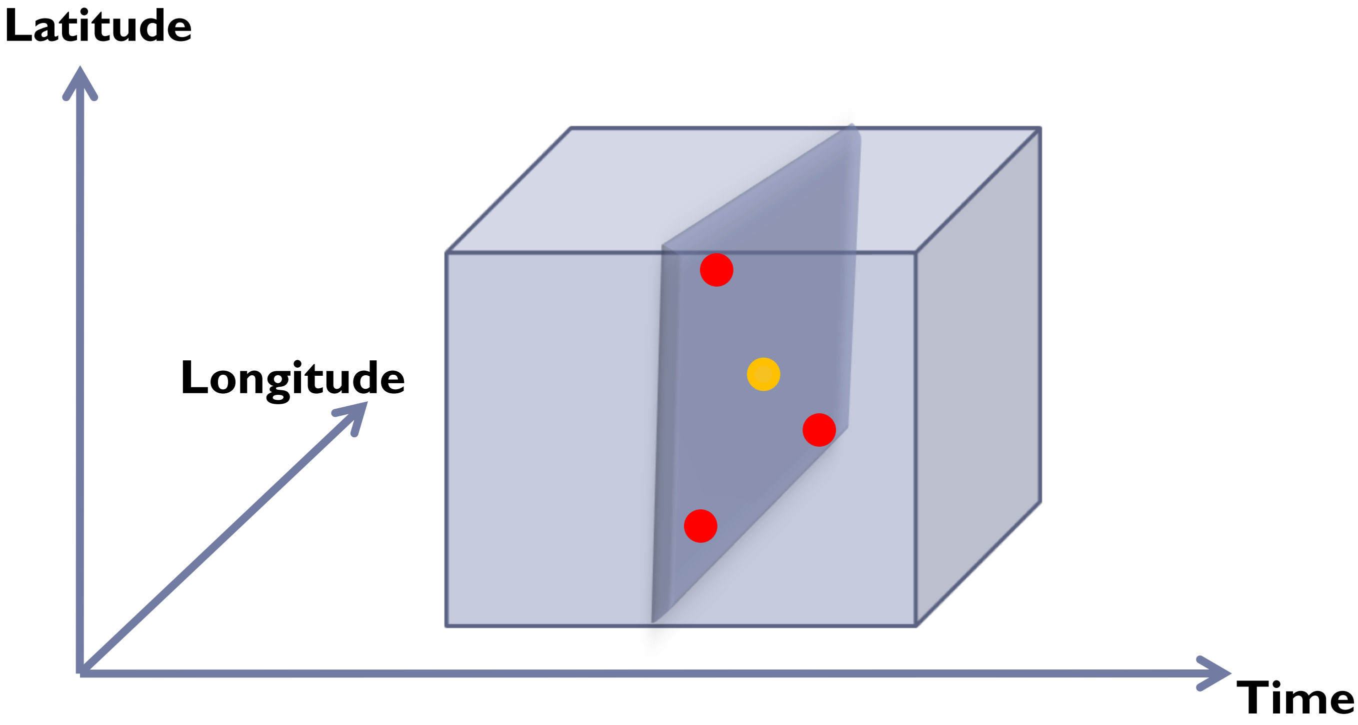
- Spatial cloaking
- Temporal cloaking



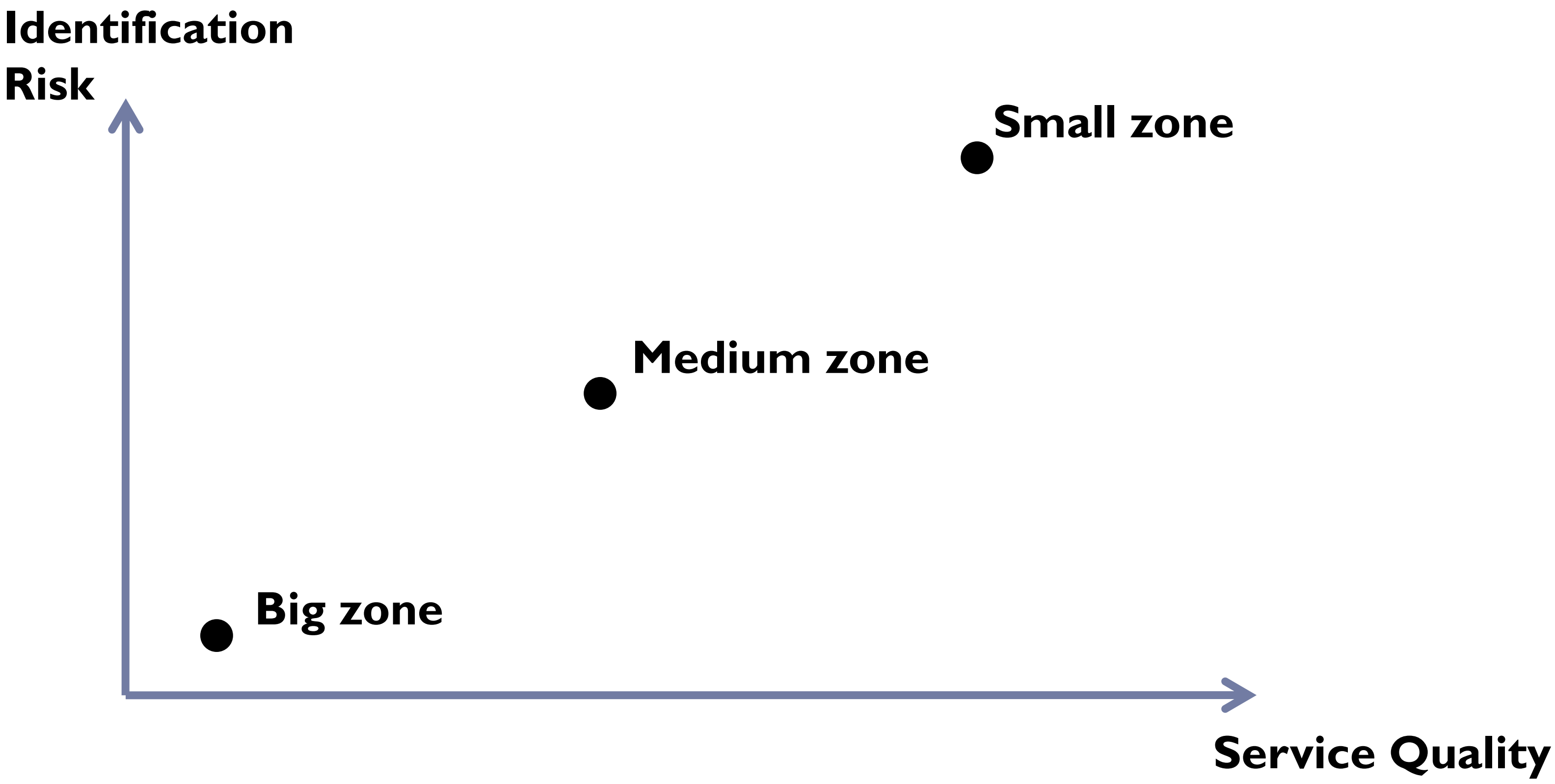


Defenses: Spatio-temporal cloaking

- Spatial cloaking + temporal cloaking



Anonymization Trade-off



Not yet there…

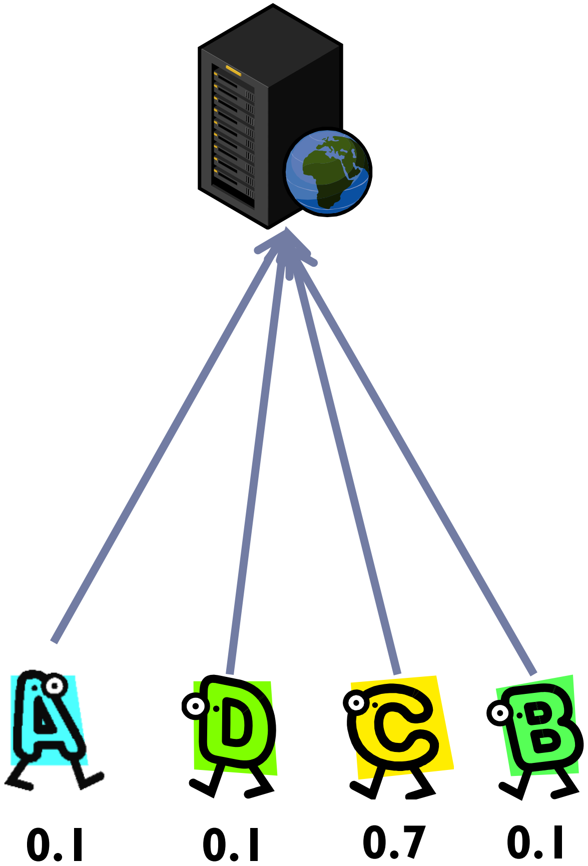
- How to anonymize?
  - Optimize tradeoff
- Which is the best architecture?
  - All have problems
  - Authentication! Anonymous credentials are slow...
- How do we measure privacy?
  - Is k-anonymity the best we can do?
- Location-based services develop faster than research...

Anonymity metrics

What counts for anonymity?

- Definition of anonymity
  - *Anonymity is the state of being not identifiable within a set of subjects, the anonymity set.*
  - The *anonymity set* is the *set of all possible subjects who might cause an action or be addressed.*

- Anonymity depends on:
  - The number of subjects in the anonymity set
  - The probability distribution of each subject in the anonymity set being the target



Entropy: information-theoretic anonymity metrics [DSCP02, SD02]

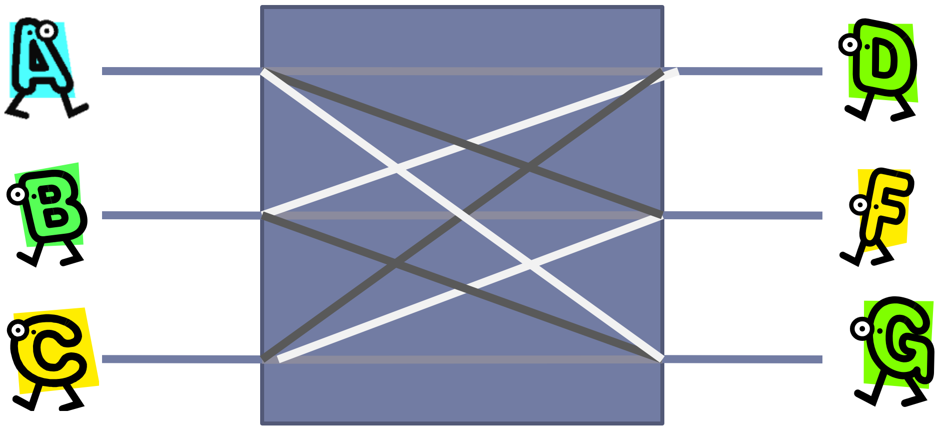
- Entropy: measure of the amount of *information* required on average to describe the random variable
- Measure of the *uncertainty* of a random variable
- Increases with N and with uniformity of distribution

$$H = -\sum_{i=1}^{N} p_i \cdot \log_2 (p_i)$$

- Distribution with entropy H equivalent to uniform distribution with 2^H subjects
- Other information theoretic metrics: min-entropy, max-entropy, Rényi entropy, relative entropy, mutual information, ….

Combinatorial approaches

- Edman et al.
  - Consider deanonymization for a system as a whole (instead of individual users)
  - Find perfect matching inputs/outputs
  - Perfect anonymity for *t* messages: *t!* equiprobable combinations



Conclusions

- Privacy is not “opposed” to security, but rather a security property

- Soft Privacy is the state of the art in development
  - Hidden costs of securing the data silos
  - Hidden costs of public image

- Hard Privacy solutions:
  - e.g., Credentials, Anonymous communications
  - Poor deployment (cost)

- The new challenge: Location privacy

More topics

- Database privacy
- Social networks
- Privacy policies
- Censorship resistance
- Economics of privacy and surveillance

Further reding

- Books
  - Daniel J. Solove ,“Understanding privacy”
  - A. Pfitzmann and M. Hansen,“Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management - a consolidated proposal for terminology”
  - W. Diffie and S. Landau,“Privacy on the line”

- Articles
  - G. Danezis and C. Diaz,“A Survey of Anonymous Communication Channels”
  - J. Krumm,“A Survey of Computational Location Privacy”

Ask me

carmela.troncoso@esat.kuleuven.be