Advanced Network Security

Anonymity

Amir Mahdi Sadeghzadeh, Ph.D.

Most slides have been adapted from Mehdi Kharrazi, CE40-817, Sharif University of Technology, 2015

Privacy on Public Networks

- Internet is designed as a public network
  - Machines on your LAN may see your traffic, network routers see all traffic that passes through them
- Routing information is public
  - IP packet headers identify source and destination
  - Even a passive observer can easily figure out who is talking to whom
- Encryption does not hide identities
  - Encryption hides payload, but not routing information
  - Even IP-level encryption (tunnel-mode IPsec/ESP) reveals IP addresses of IPsec gateways

Privacy

- We take privacy in our daily lives for granted
- In the internet that is not the case
- Examples:
  - Pentium III chip serial numbers
    - Read via software (ActiveX or Applets)
    - Helps track a user over the web
    - After pressure from privacy activists Intel decided to turn it off by default
    - Could be turned on by software

Privacy

- Cookies
  - Used to keep a track of the sites you visit
  - double-click and other advertising agencies are main employers of cookies
- Carnivore sniffer
  - Employed by the FBI
  - Almost all emails can be scanned in real time
  - You could encrypt your message

Ways to Achieve Privacy

- Encryption
  - Privacy of content
- Anonymity
  - Privacy of connection

- Compromised end nodes could expose everything

Outline

- Terminology
- Definition
- Anonymous Methods
  - Mix-net
  - DC-net
  - Crowds
  - Onion Routing

What is Anonymity?

- Anonymous
  - of unknown authorship or origin, lacking individuality, distinction, or recognizability <the anonymous faces in the crowd>
    - Merriam-Webster's Collegiate Dictionary

Terminology

- Terminology proposed by Pfitzman and Kohntopp
- Anonymity is the state of being not identifiable within a set of subjects, the anonymity set.
  - i.e. A sender will be anonymous among the set of possible senders, the same argument goes for the recipient.
- The attacker never forgets anything so the anonymity set never increase for the attacker but decreases or has no change.
  - But if misinformation is used one would be able to introduce uncertainty into the system thus increase the anonymity set.

Terminology

- Unlinkability of two or more items (e.g., subjects, messages, events, actions, ...) means that within this system, these items are no more and no less related than they are related concerning the a-priori knowledge.
- Unobservability is the state of Item of Interest (IOI) being indistinguishable from any IOI at all.
  - IOI include a subject, event, action (e.g., send, receive, move, etc), specific type of messages

- Anonymity could be resulted from Unobservability.

Aspects of Anonymity

- Pfitzman and Waidner in 1997
- Two Aspects:
  - Types of anonymity
    - Sender Anonymity
    - Receiver Anonymity
    - Unlinkability of sender and Receiver
- Model of the attacker
  - Anonymity with respect to an attacker

Informal Definition

- Crowds
- Reiter and Rubin 1998
- Added a third aspect to anonymity
  - Degree of Anonymity

Informal Definition

- Absolute Privacy means that the attacker has no way to distinguish the situation in which a potential sender actually sent communication and those in which it did not.
- Beyond Suspicion means that the attacker can not distinguish between a set of possible senders.

Informal Definition

- Probable Innocence if in the attackers point of view, the sender appears no more likely to be the originator
- Possible Innocence from the attackers point of view if there is a nontrivial probability that the real sender is someone else.

Informal Definition

- Exposed if from the attackers point of view there is a high probability about who the sender is.
- Provably Exposed if the attacker can identify the identity of the sender and prove it to everyone else.

Defining Anonymity

- Shields, and Levine 2000
- Let PI(x) be the probability the entity x is the initiator. Also let x be a member of a non-empty set S, assuming equiprobability
- The degree of anonymity is

$$\sum_{y \in S} p_I(y) = 1$$

$$d_x = 1 - p_I(x)$$

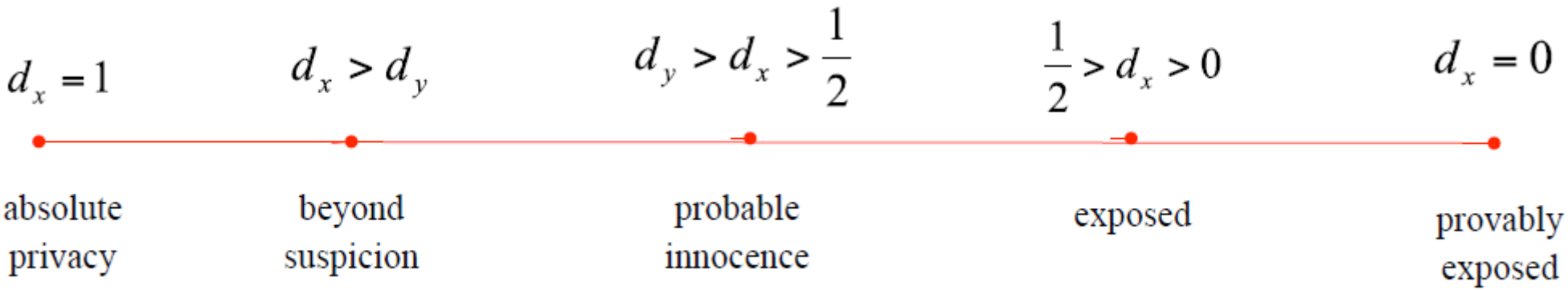
$$d_x = \sum_{y \in S \neq x} p_I(y)$$

- Since all members of S have an equiprobable chance of being the initiator

$$d_x = 1 - \frac{1}{|S|}$$

Informal Definition

- Absolute Privacy when the attacker can not perceive the presence of communication, |S|= ∞ and dx=1
- Beyond Suspicion when x appears no more likely to be the initiator than any potential entity in the system, dx> dy
- Probable Innocence if x appears no more likely to be the initiator than not to be the initiator, but x appears more likely than all othe entities 1/2<dx<dy
- Exposed if there exist a possibility that x is not the initiator 0<dx<1/2
- Provably Exposed if the attacker can prove x is the initiator, dx=0

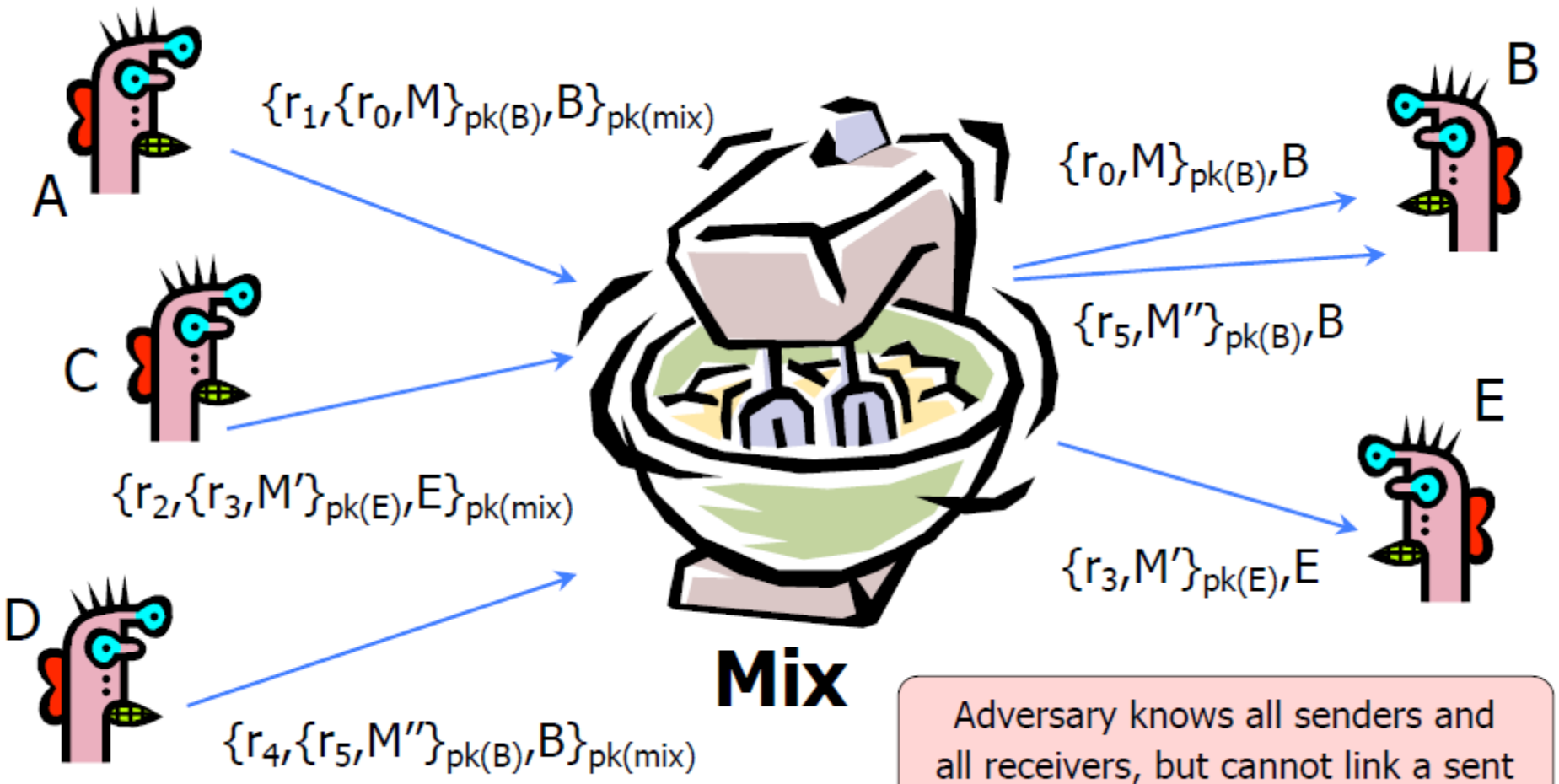


MixNets

Mix-net

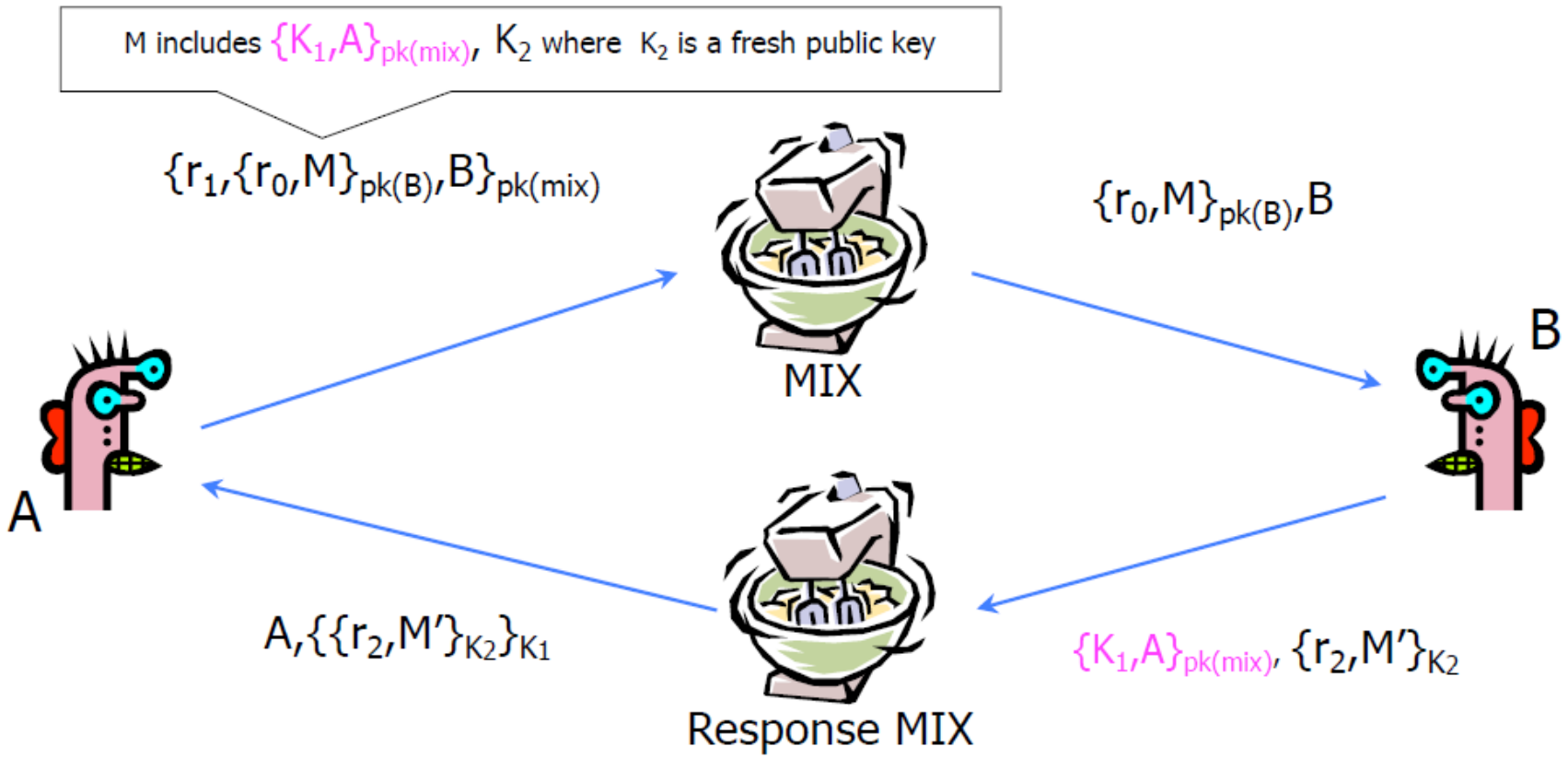
- Untraceable electronic mail, return addresses, and digital pseudonyms
- Chaum 1981
- Two Assumptions:
  - No correlation between a set of sealed and unsealed items
  - Anyone may learn the origin, destination and representation of all messages and may inject, remove, or modify messages

Basic Mix Design



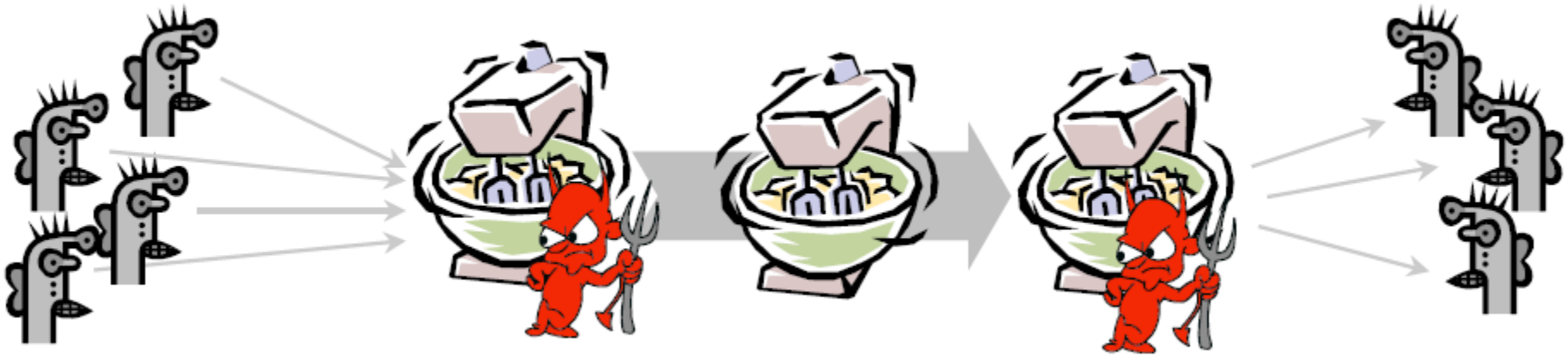
Adversary knows all senders and all receivers, but cannot link a sent message with a received message

Anonymous Return Addresses



Mix Cascade

- Messages are sent through a sequence of mixes
  - Can also form an arbitrary network of mixes (“mixnet”)
- Some of the mixes may be controlled by attacker, but even a single good mix guarantees anonymity
- Pad and buffer traffic to foil correlation attacks



Mix-net

- No item which is repeated in the input should be allowed to be repeated in the output
  - Solution, make sure the nonce has some correspondence to time
- Depends on security of public key system
- Good for Periodic deliveries
- Has high Latency

DC-Nets

DC-net

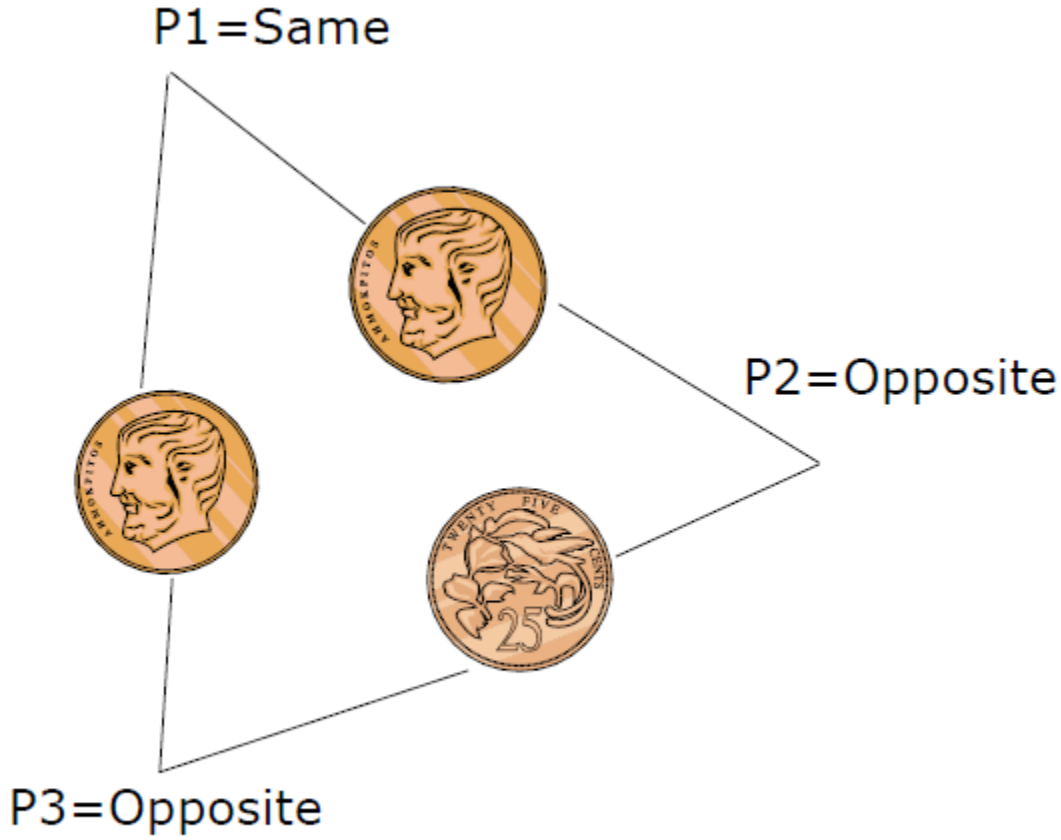
- The dining cryptography problem: unconditional sender and recipient untraceability
- Chaum 1988
- 3 cryptographers in a restaurant wonder if they are paying the bill or the NSA

DC-net

- So they each toss a coin, and then each says out loud if his and the person to his right coin landed on the same side
- If he was the payer he states the opposite
- An even number of differences means NSA is paying and odd number means otherwise

DC-net (example)

- Since the number of differences is even NSA has paid the bill
- If P2 had paid it would announce “same” and then the number of differences would be odd



Superposed Sending

- This idea generalizes to any group of size N
- For each bit of the message, every user generates 1 random bit and sends it to 1 neighbor
  - Every user learns 2 bits (his own and his neighbor's)
- Each user announces own bit XOR neighbor's bit
- Sender announces own bit XOR neighbor's bit XOR message bit
- XOR of all announcements = message bit
  - Every randomly generated bit occurs in this sum twice (and is canceled by XOR), message bit occurs once

Crowds

Crowds

- Proposed by Reiter (Bell Labs) and Rubin (AT&T Labs) in 1997
- Basic Idea:
  - “Blending into a Crowd,” i.e., hiding one’s actions within the actions of others.
- Static paths

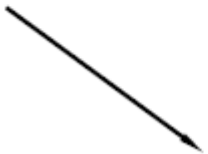
- The main idea
  - hide each user's communications by routing them randomly within a group of similar users.
    - Neither the collaborating group members nor the end receiver can therefore be sure where in the group the packet originated.

What makes up a Crowd network?

- Path length depends on:
  - Probability of forwarding
- Data encrypted over the links but in clear at the node

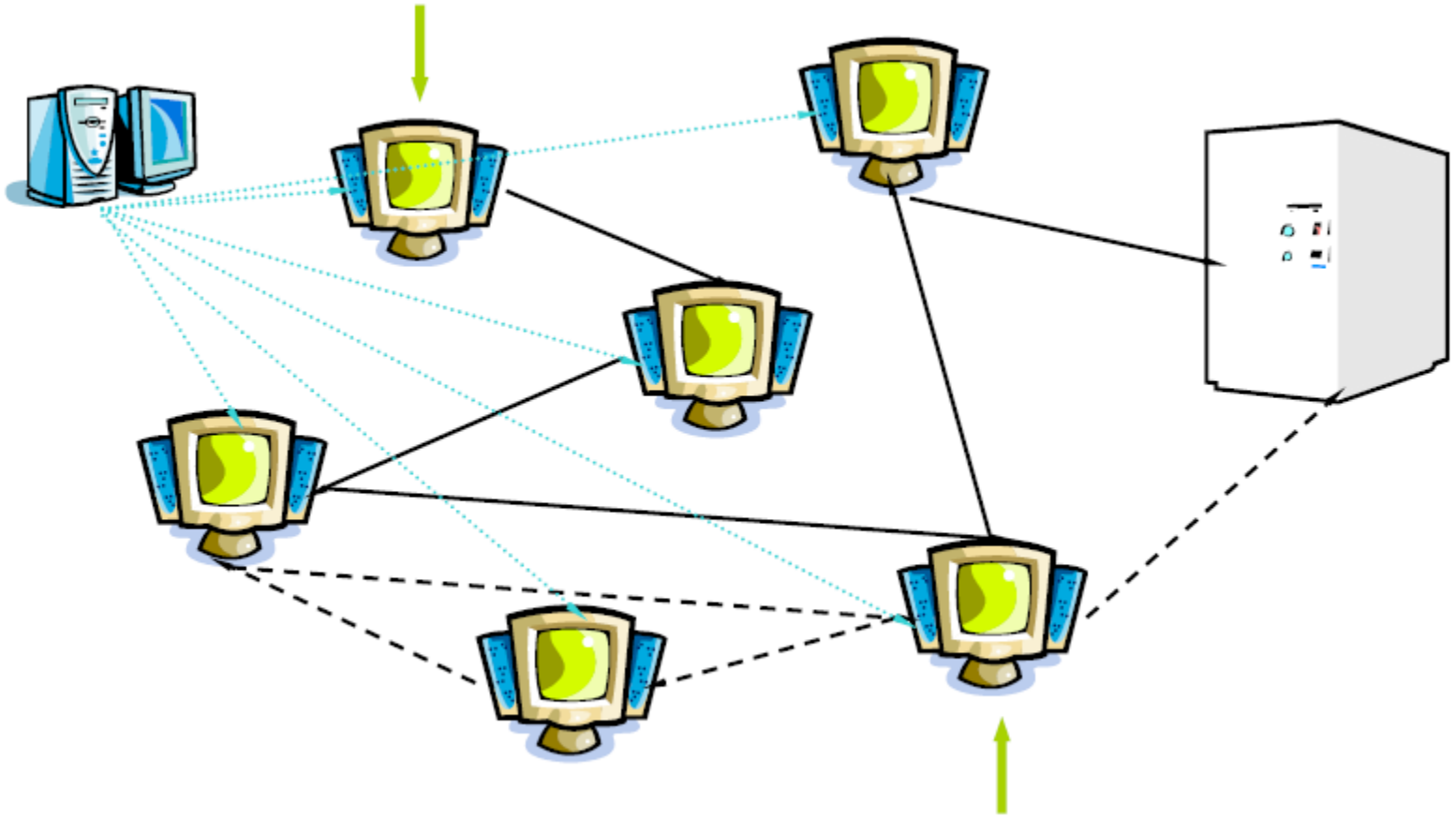
John Doe

Blender



Link Keys

Crowds Example



How crowds works

1. Each user joins a crowd of other users by registering himself at the blender which is a single server responsible for membership management. When a user registers, all the other members in the crowd are notified. The blender is also responsible for key distribution, as it distributes symmetric keys to individual pairs of jondos, used for encryption and decryption, respectively of packets routed along the virtual paths.
2. Each user is represented by a jondo on her machine which is an application that runs on a user's computer.
3. Each jondo either submits a request to the end server or forwards it to a randomly chosen jondo (possibly itself). Other jondo tasks are to strip out any personal information such as cookies, identifying header fields.
4. A jondo cannot tell if a request is initiated by the previous jondo or one before it.
5. Request and reply follow the same virtual paths which are constructed using an algorithm involving probabilities. The virtual paths are torn down and reconstructed on a regular basis to allow anonymity for newly added members.

Crowds

- Based on UDP
- Designed for web traffic
- Short lived web connection
- No link padding
- Anonymity as good as anonymity of data stream
- Slow crowd member slow network
- Can’t join at anytime

Onion Routing

Onion Routing

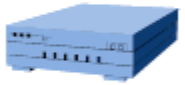
- Anonymous Connections and Onion Routing
- Reed, Syverson, and Goldschlag 1997
- http://www.onion-router.net/
- Real-time Chaum mixes
  - Called onion network

What makes up an onion network?

Application Proxy

Onion Proxy

Entry or Exit funnel



Onion Router

Onion

ACI (Anonymous Connection Identifier)

Onion Routing

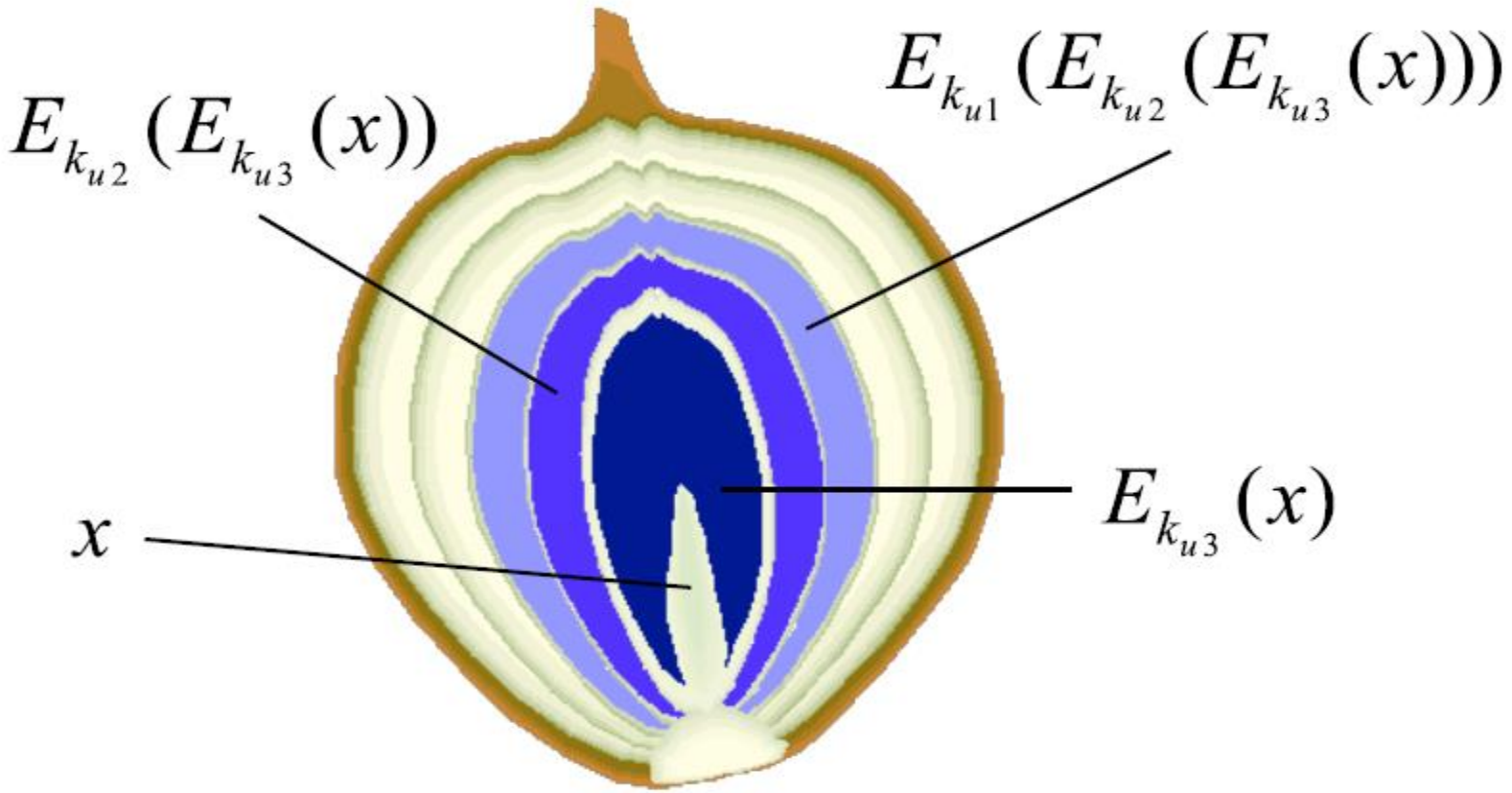
- 3 phases
  - Connection setup
    - Public key system is used
    - ACIs are made
  - Data delivery
    - Symmetric encryption used for speed
    - Received packets in a fixed time interval by a mix are Randomly reordered
  - Connection termination

Onion Routing

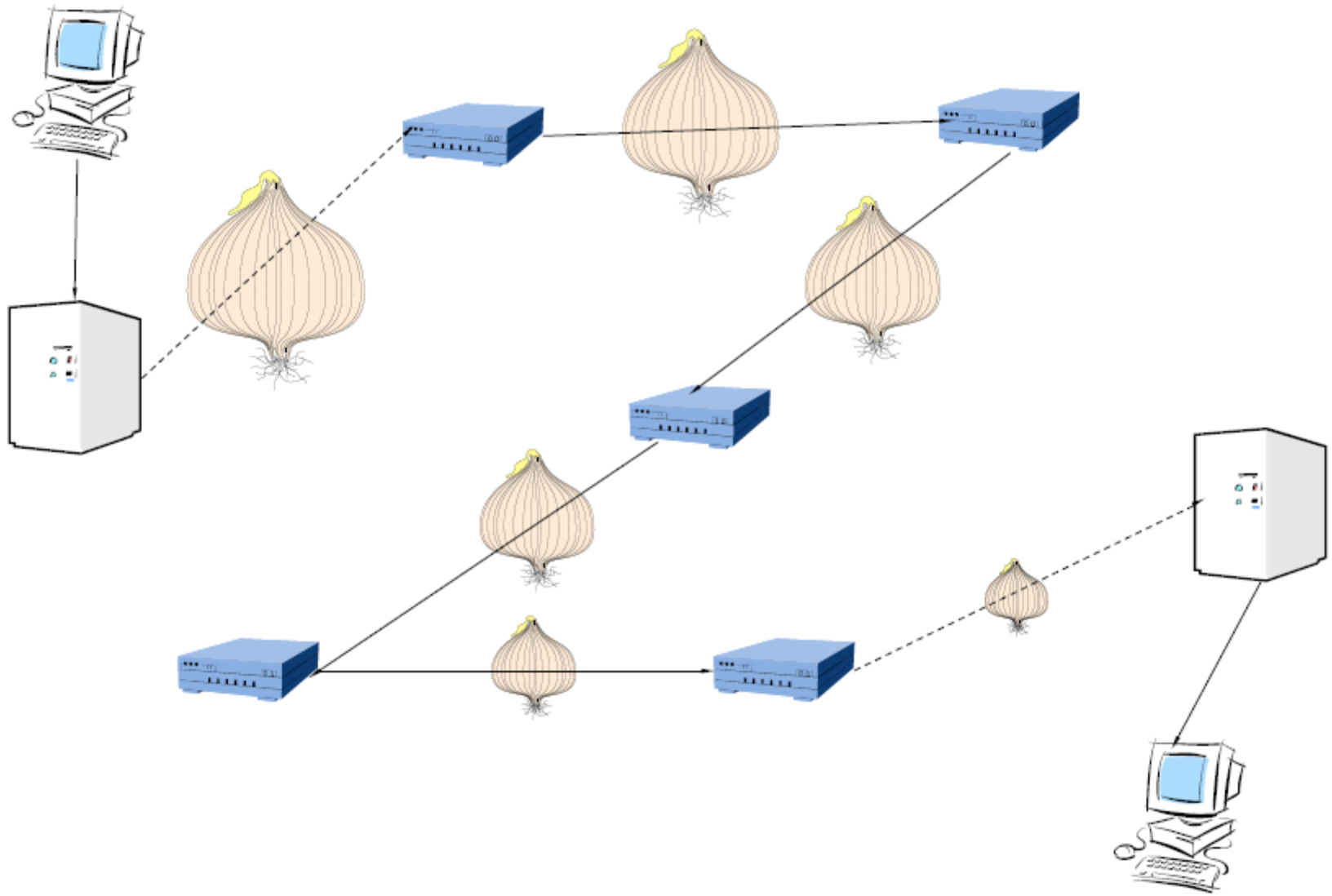
- Uniform sized cells of 128 bytes
  - Use of padding to maintain fix size
  - Because of cell size, route limited to maximum of 11 nodes
- Lower Limit on traffic flow
  - To avoid data burst attacks
- The network is intended for real time traffic

Onion details

- Were k_u is the public key of the onion routers
- The first encryption is done using the key of that last router and so on.



Onion Routing Example



Onion Routing

- Based on TCP/IP
- 2 separate functions:
  - Anonymity of connection
  - Anonymity of data stream
- Real-time capability
- Link padding

Acknowledgments/References

- [Shmatikov] CS 378 - Network Security and Privacy, Vitaly Shmatikov, University of Texas at Austin, Fall 2007.
- David L. Chaum, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Communication of the ACM, Vol. 24, No. 2, Feb 1981
- Pfitzaman, A. and Waidner, M. 1987. Networks without user observability. Computer Security 2, 6, 158-166
- Marit Kohntopp, and Andreas Pfitzman, Anonymity, Unobservability, and pseudonymity-A Proposal for Terminology, Draft v.012 June 17, 2001
- David L. Chaum, The dining cryptographers problem: unconditional sender and recipient untraceability, journal of cryptology, 1:56-75, 1988
- Anonymous connection and onion routing, Syverson P., Goldshlag D., and Reed M. ,IEEE Journal on Selected Areas in Communications, VOL. 16, NO. 4, MAY 1998
- Reiter M.K. and Rubin A.D. Crowds: Anonymity for Web Transactions. ACM Transactions for on Information and System Security, 1(1):66-92, November 1998.