

Document Leakage

John Maheswaran

Crypto-Book: integrating cryptography with social networking

- Initially investigated using Facebook as a public key infrastructure
- Implemented secure Facebook messaging using public key cryptography
- Later implemented secure Facebook messaging using Boneh-Franklin identity based encryption
- Current and planned work investigates social networking with anonymity networks

www.crypto-book.com

Crypto-Book

Welcome to Crypto-Book!

Send secure Facebook messages without Mark Zuckerberg snooping on you

Choose either [identity based encryption \(IBE\)](#) (easier to use) or [public key crypto](#)

Identity Based Encryption »

Send messages straight away, no setup required.

Public Key Crypto »

If you're oldschool. Quick and easy setup.

About

Crypto-Book was created by John Maheswaran, a Yale PhD student in computer science as part of the [Dissent project](#).

If you have any questions/comments, get in touch!

john.maheswaran@yale.edu

Crypto-Book: Secure Facebook messaging

John Maheswaran

slideshare 1 / 2

[Download slides \[pdf\]](#)

Crypto-Book

- Crypto-Book: Whistle blowing through social networks
- A system to allow users to leak document anonymously
- Integrated with Facebook
- Conscript other users without their consent into a group of potential sources

Background

- The internet facilitates wide scale whistle blowing
- Sites like WikiLeaks have received large amounts of press coverage
- Major leaks include
 - Diplomatic cables
 - Iraq war documents and videos
 - Guantanamo Bay files



The Problem

- WikiLeaks faces two conflicting challenges:
 - Want to preserve anonymity of whistle blowers
 - Need to verify credibility of leaks



Protecting anonymity is critical

- Bradley Manning, an army intelligence analyst is suspected of leaking sensitive information to WikiLeaks
 - Has been arrested and faces up to 52 years and could even face the death penalty



Leak verification

- Also need to verify leak credibility
- Ideally would like to know leak comes from a credible source
- WikiLeaks currently manually verifies leaks using traditional journalistic methods

Crypto-Book

- Aims to solve the problems of preserving anonymity whilst verifying source credibility
- The document can be verified as coming from one of N sources
 - but no one knows which one
- Potential sources are linked to Facebook profiles

Crypto-Book – system flow

- User logs in with Facebook
- Authenticates with Crypto-Book servers through OAuth protocol
- Whistle blower selects a group of other Facebook profiles who will form the anonymity set
- Crypto-Book obtains public keys for each person
 - Identity based or generate 1 key for each person

Crypto-Book

- Public keys sent to user, along with user's private key
- User signs document using linkable ring signature
- Signed document is sent through anonymity network (Dissent or ToR)
- Document is submitted to publication server

Crypto-Book

- Publication server collates leaks and periodically publishes blocks of them
 - Mitigates intersection attacks
- Publication server submits signed leaked document to WikiLeaks, and links to the document through Twitter

Example use case

- President Levin says growing CS student numbers has increased costs and has meant that the CS department is no longer economically viable
- Levin decides that before he leaves office, he will drastically downsize the CS department
- Levin sends a confidential memo to all CS faculty outlining the planned downsizing

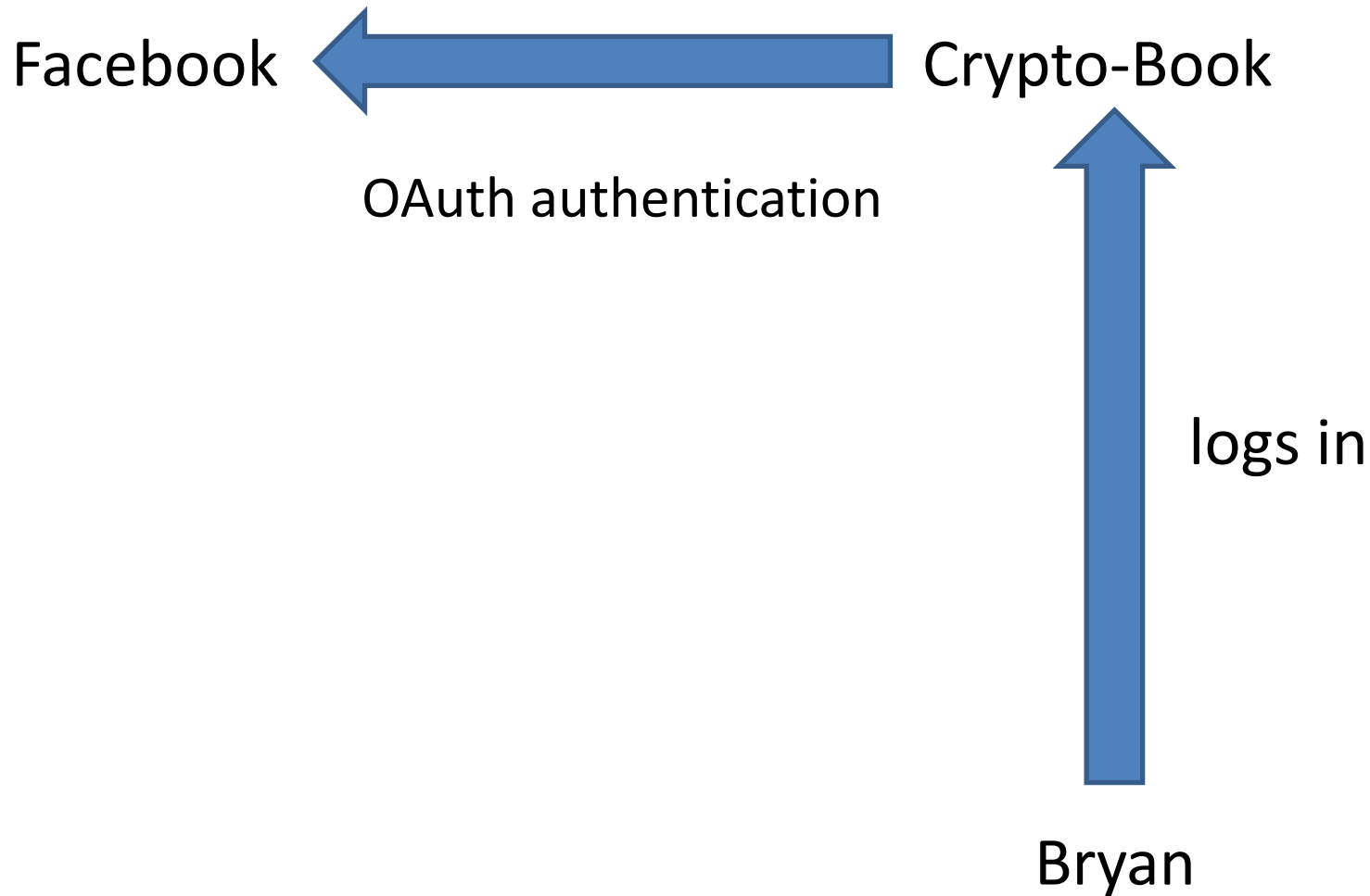
Example use case

- Bryan Ford receives the memo and is outraged at the decision
- To raise support against the plans, he wants to make the information public
- He is worried if he forwards it to the Yale Daily News, he may be indentified as the source and he might not get tenure

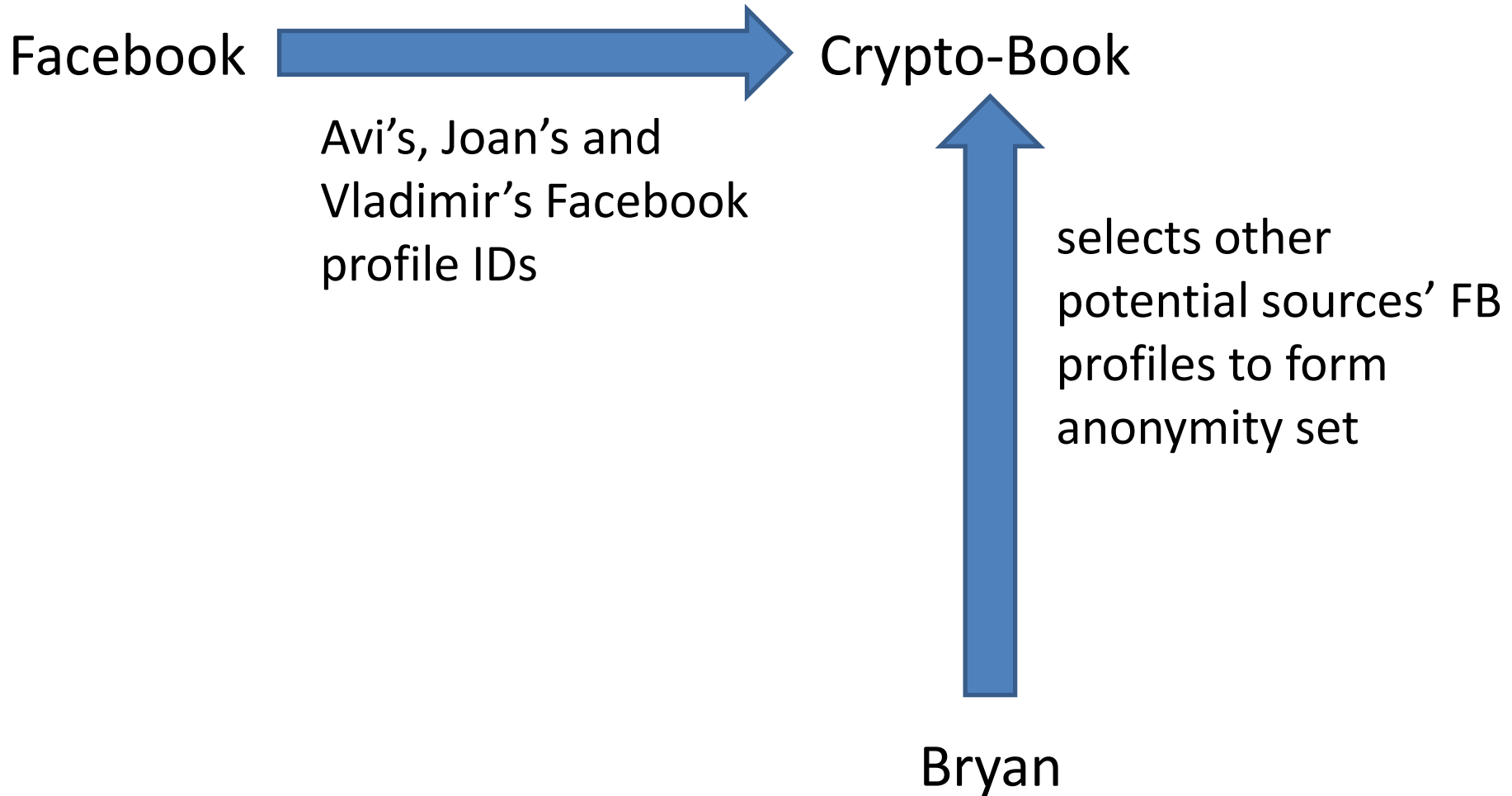
Example use case

- However if he anonymously leaks the email, people might not believe the story
- He decides to use Crypto-Book to get the word out.....

Bryan wants to leak Levin's memo



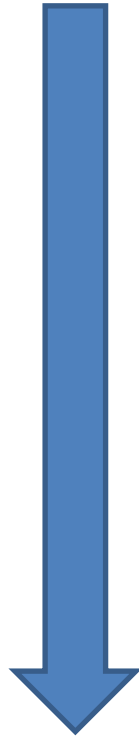
Choosing the anonymity set



Bryan obtains keys

Crypto-Book

Generates key pair for each user using identity based or other generation scheme



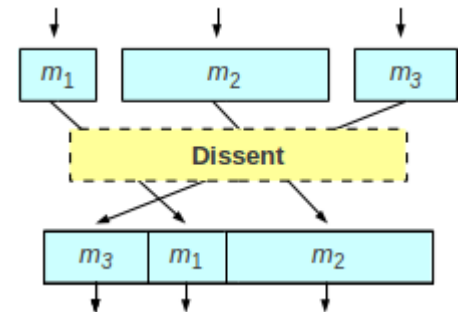
Avi, Joan, Vladimir
and Bryan's public
keys
Bryan's private key

Bryan

Bryan signs and leaks memo

Bryan

3. Submits signed document to anonymity network



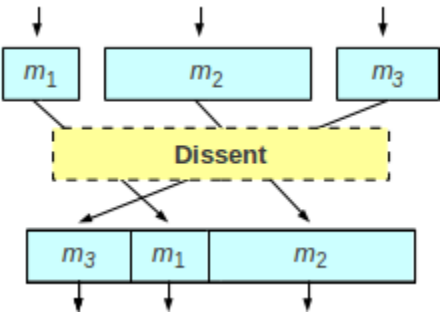
1. Creates a linkable ring signature (LRS) using Avi, Joan, Vladimir and his own keys
2. Signs Levin's memo using LRS



Design option

- May be able to use Deniable Anonymous Group Authentication (DAGA) instead of linkable ring signatures to provide forward anonymity
 - Even if someone later hacks Bryan's Facebook account, they cannot identify him as the source of the leak

Memo sent to publication server



Leaked signed memo



Publication server

Publication server waits until it has several leaks with overlapping anonymity sets (to mitigate intersection attacks)

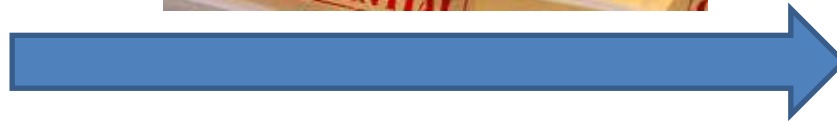


Document is made public

Multiple leaked documents



Publication server



Once many leaks have been received, publication server publishes them



Outcome

- Yalies see Levin's memo on WikiLeaks or linked to from Twitter
- Linkable ring signature allows people to verify the authenticity of the leak
 - The memo came from either Vladimir, Bryan, Joan or Avi, so know the source is credible
 - But no one knows who exactly leaked it
- Levin is annoyed that his memo was leaked, but cannot punish all four professors
- In face of student protestation, Levin retracts his planned downsizing of the CS department

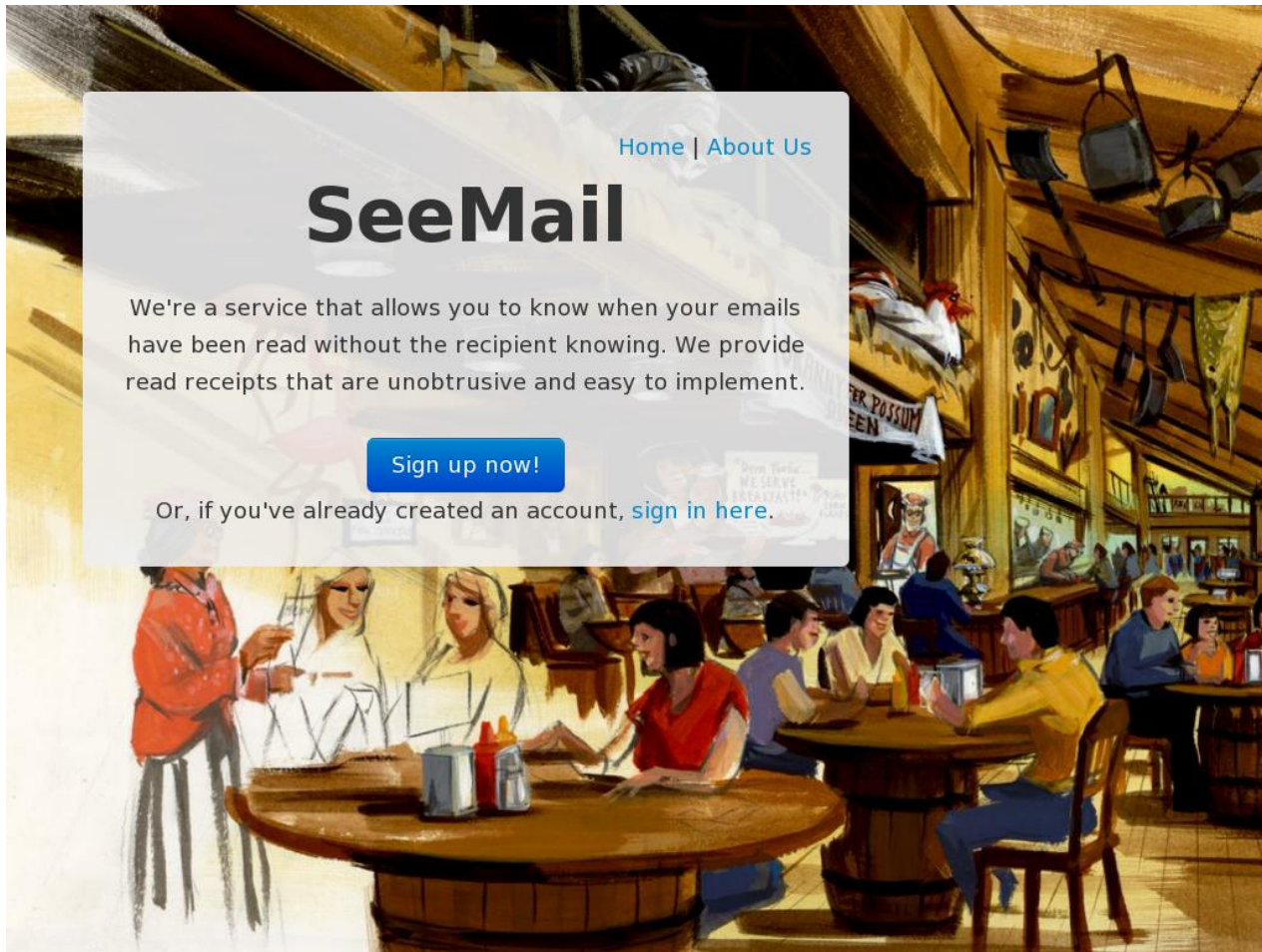
SeeMail – the problem

- Companies want to keep track of their sensitive data
- Want to mitigate data leaks, identify leak sources and track who data is leaked to
- Average cost of a data leak at between \$90 and \$305 per lost record [Forrester Research]
 - legal representation, PR expenditure, costs to have systems externally audited, loss of reputation and monitoring credit reports of consumers if financial information is leaked

SeeMail

- Idea is to track when emails are read and forwarded using email beacons
- Email beacons are unique images and each time one is loaded, it is logged

SeeMail - www.seemail.me



[Home](#) | [About Us](#)

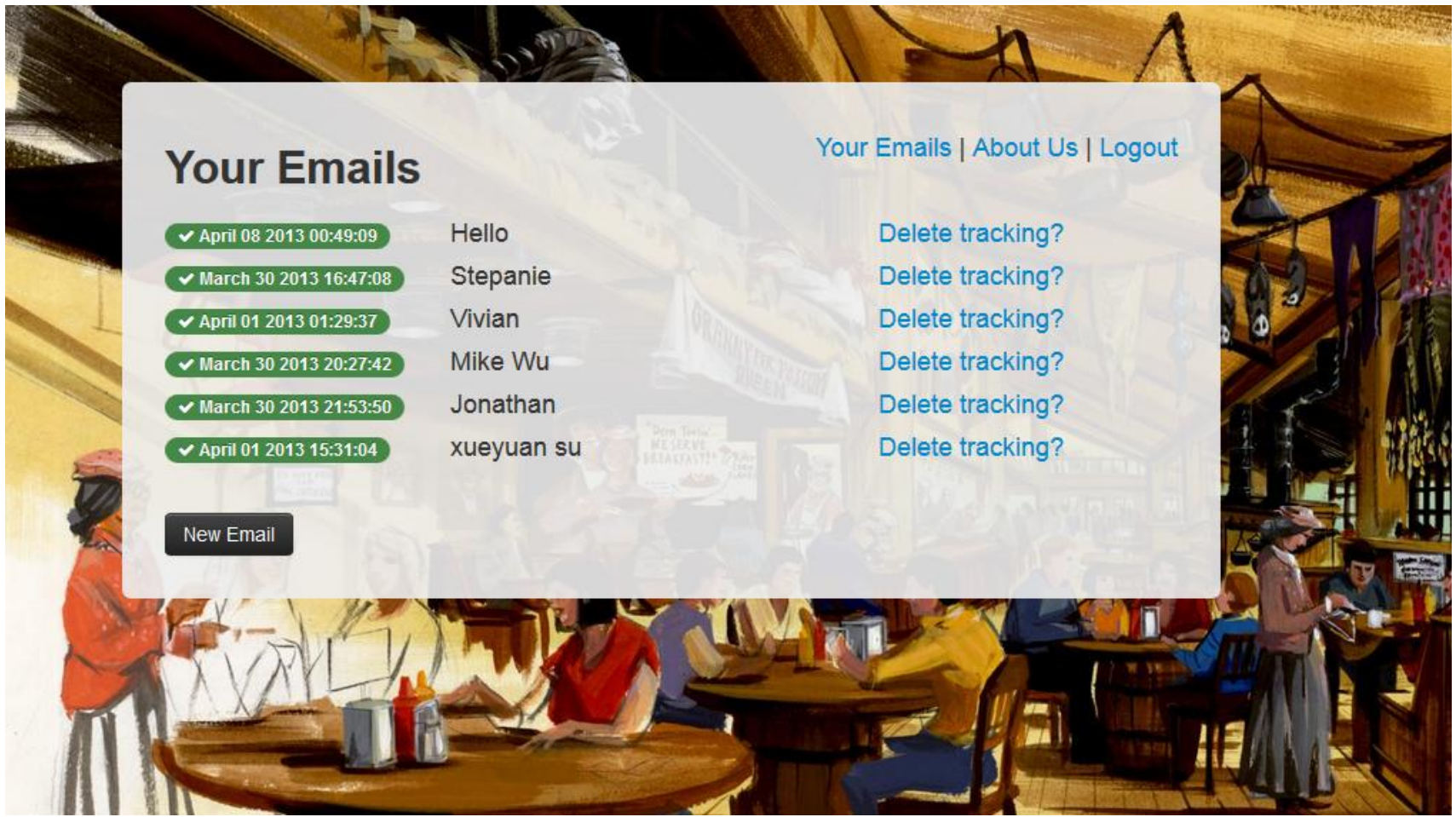
SeeMail

We're a service that allows you to know when your emails have been read without the recipient knowing. We provide read receipts that are unobtrusive and easy to implement.

[Sign up now!](#)

Or, if you've already created an account, [sign in here](#).

SeeMail - www.seemail.me



Your Emails

[Your Emails](#) | [About Us](#) | [Logout](#)

✓ April 08 2013 00:49:09	Hello	Delete tracking?
✓ March 30 2013 16:47:08	Stepanie	Delete tracking?
✓ April 01 2013 01:29:37	Vivian	Delete tracking?
✓ March 30 2013 20:27:42	Mike Wu	Delete tracking?
✓ March 30 2013 21:53:50	Jonathan	Delete tracking?
✓ April 01 2013 15:31:04	xueyuan su	Delete tracking?

[New Email](#)

Future work

- Want to track IP addresses and geolocate users
- iPhones support display of iframes in emails
 - Hope to covertly extract more information from user
 - May be able to use Java script side channel attacks to see what other apps the user is running
 - May be able to extract GPS location of user when they read the email
 - Eventually hope to perform user study to see what proportion of iPhone users we can extract private information from

Future work – Anti-SeeMail

- SeeMail techniques may be misused by oppressive regimes to silence whistle blowers
- Hope to look at ways to guard against email tracking
- Compare email objects with peers and clean any potentially unsafe ones before leaking the document

Future work – Anti-SeeMail

- Want to look at Anti-SeeMail for web browsers
 - Have a pool of anonymous browsers that fetch web pages and compare them
 - Clean out any user specific parts such as web bugs, tracking scripts, targeted ads
 - Then display cleaned version to the end user