An Offline Foundation for Accountable Pseudonyms

Bryan Ford **Jacob Strauss**

MIT CSAIL

SocialNets

April 1, 2008

Introduction

- Anonymity is a cherished principle
  - Traditional: voting, peer review
  - Online: email, polls
- But comes with a steep cost?
  - Traditional: ballot stuffing
  - Online: Poll stuffing, Spam
  - Sybil Attacks

Wrong Approach

- Pervasive Identification
  - Tradeoff between anonymity and accountability?
  - Leads to a big-brother society
- Disposability, not Anonymity alone, is the real problem with online identity
  - Little incentive to behave if new accounts are free
  - If accounts are *not* free, then there *is* incentive to behave

Proposal: Sybil Resistance

- A basic public utility
  - Sybil protection like Fire/Police protection
  - Apply generically to many situations
    - Not just to single organization
  - Combine Online & traditional cases

Outline

- Introduction
- System Goals
- Design Sketch
- Related Work
- Summary

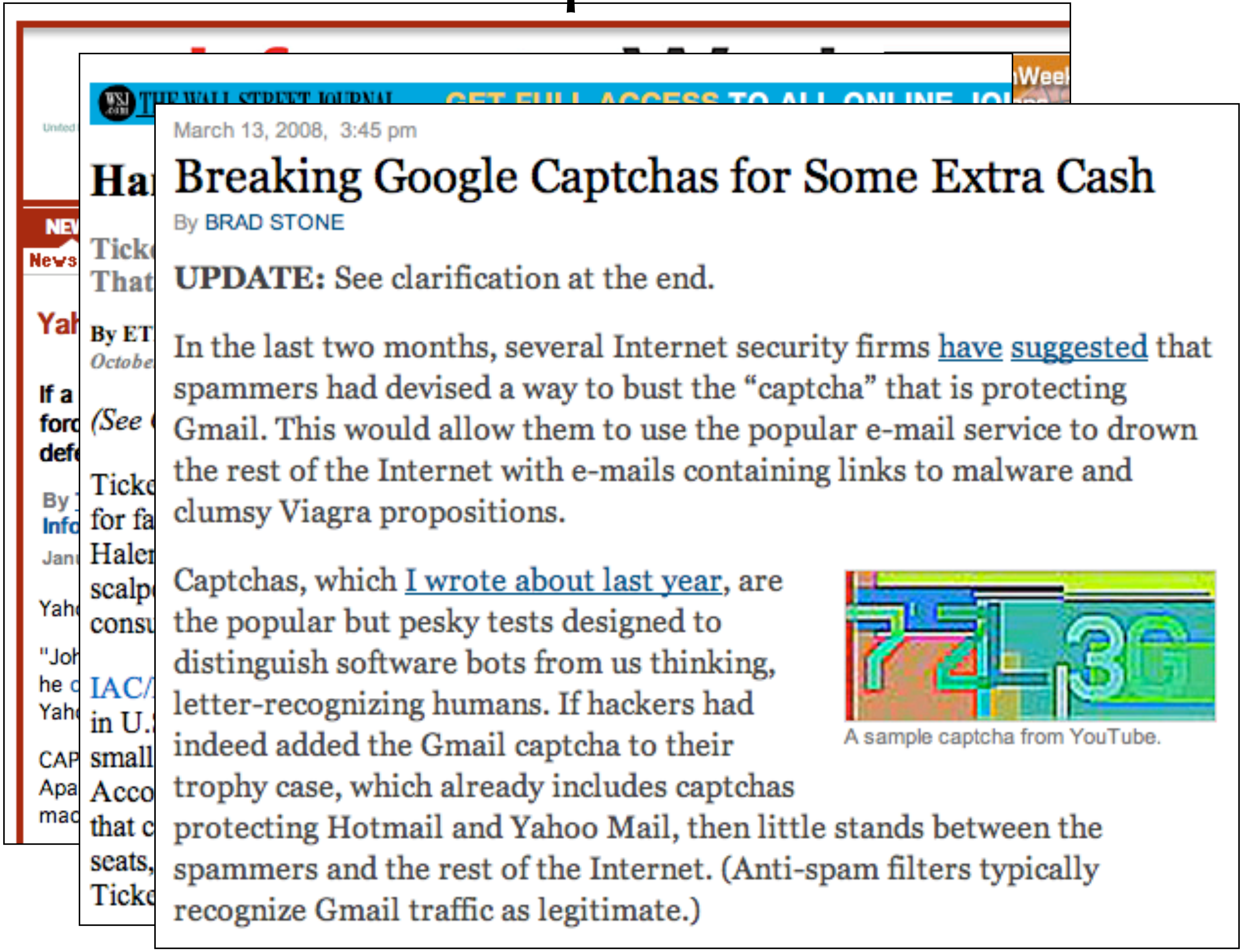
Existing Identity Allocation

- Government issued ID's
  - Social Security numbers
  - Passport, driver's license
  - Voter registration
- Purchasable resources
  - IP addresses
  - CPU time, network bandwidth
  - Cell phone numbers [gmail]
  - Credit card numbers
  - Fake IDs
  - User time to solve CAPTCHAs

Properties of existing solutions

- Too many choices
- Technical Attacks
  - Can be very bad (Spam)
- Social Attacks
  - Depends on participants, never perfect

Example Attacks



March 13, 2008, 3:45 pm

Breaking Google Captchas for Some Extra Cash

By BRAD STONE

UPDATE: See clarification at the end.

In the last two months, several Internet security firms have suggested that spammers had devised a way to bust the "captcha" that is protecting Gmail. This would allow them to use the popular e-mail service to drown the rest of the Internet with e-mails containing links to malware and clumsy Viagra propositions.

Captchas, which I wrote about last year, are the popular but pesky tests designed to distinguish software bots from us thinking, letter-recognizing humans. If hackers had indeed added the Gmail captcha to their trophy case, which already includes captchas protecting Hotmail and Yahoo Mail, then little stands between the spammers and the rest of the Internet. (Anti-spam filters typically recognize Gmail traffic as legitimate.)

A sample captcha from YouTube.

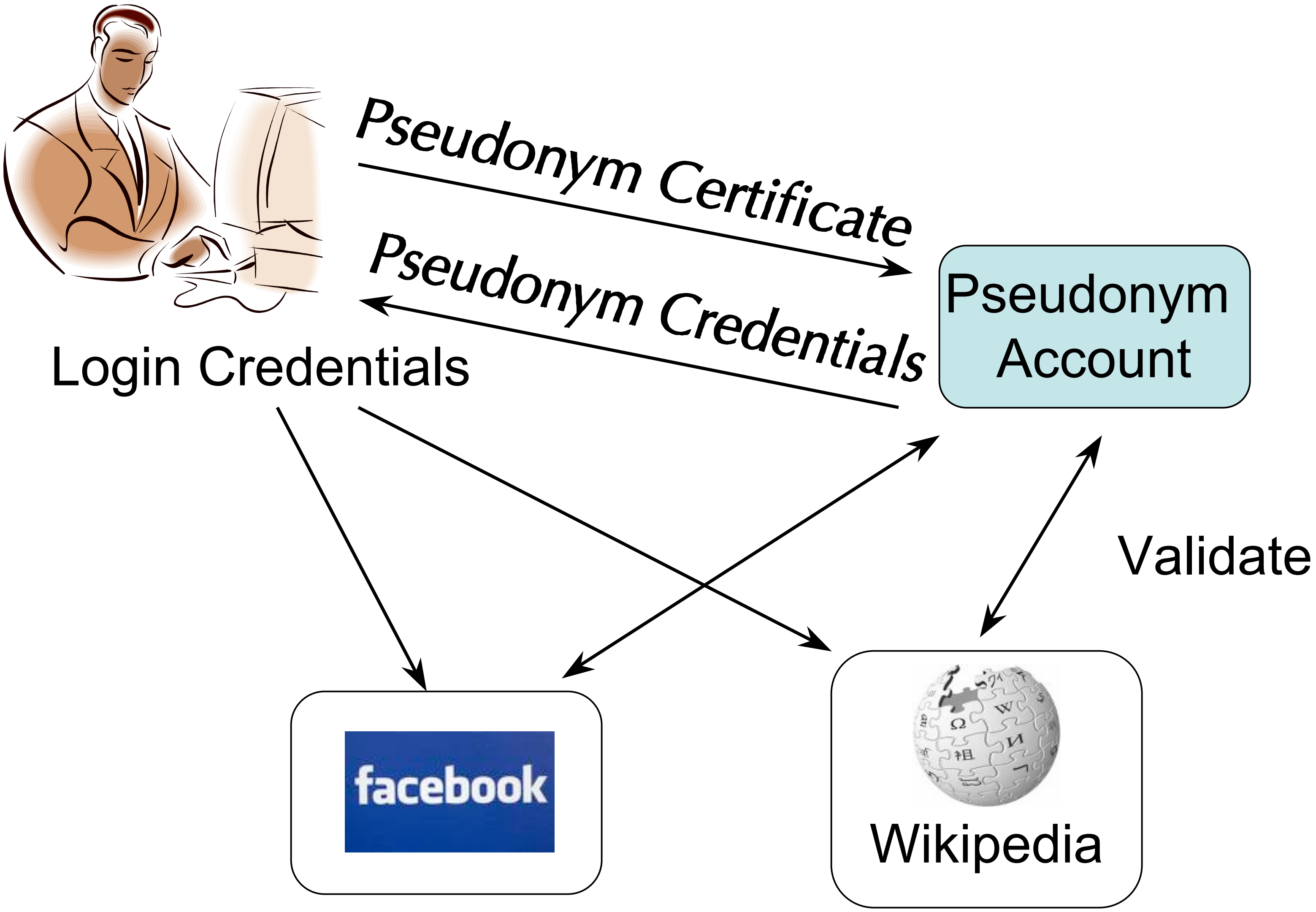
Right Approach: Accountable Pseudonyms

- Generic Public Utility
  - usable for all online services
- Make creating duplicate identities hard
- Preserve anonymity
- One body, one pseudonym per service
  - Keep link between user's pseudonyms private

An Offline Foundation for Online Pseudonyms

- Physically attend a nearby party
  - Once a year on a particular day?
- Get a paper certificate
  - Hand stamp to prevent duplicates
- Redeem certificate for one online pseudonym account
  - Acts as a generator for service-specific pseudonyms
  - Guarantees one-body, one-pseudonym property

Anonymous Single Sign on



Pseudonym Certificate

Pseudonym Credentials

Pseudonym Account

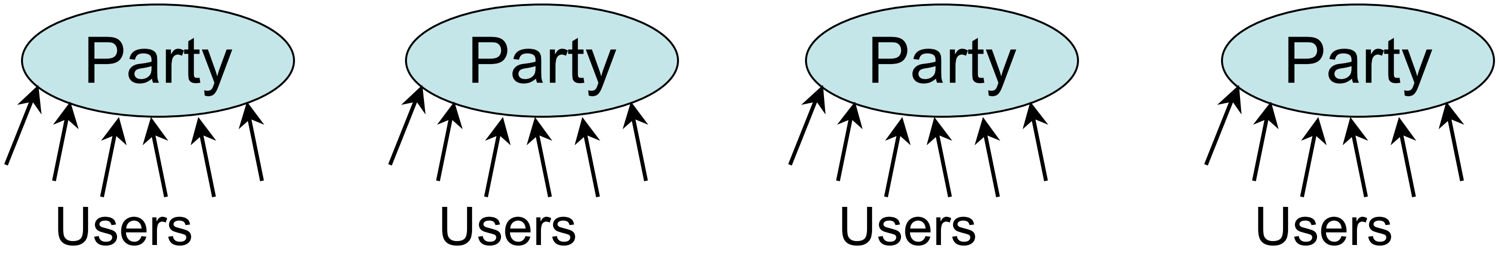
Login Credentials

Validate

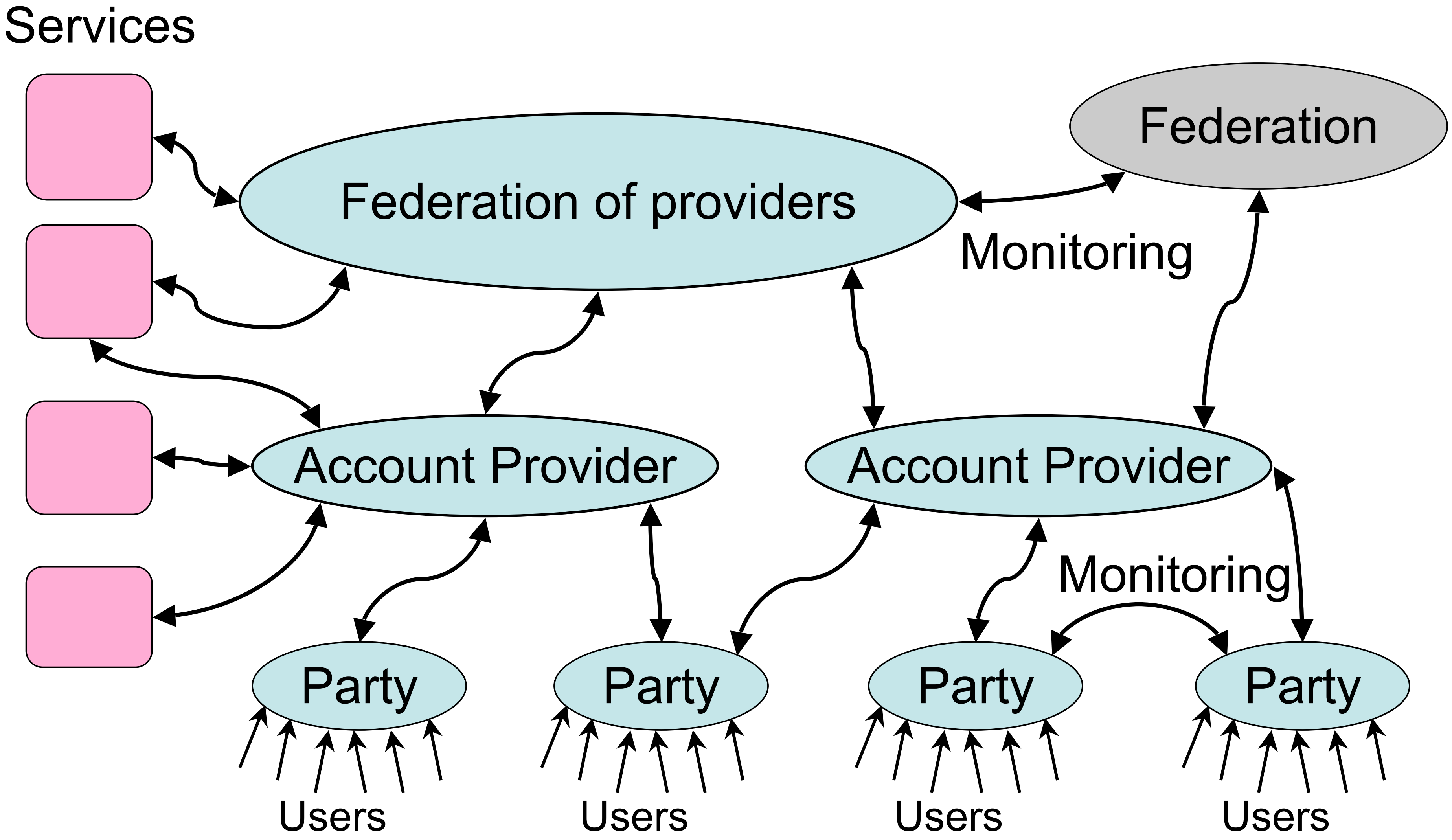
Wikipedia

Federated Parties

- Need many parties so that everyone can find one to attend



Federated Parties



Trust Relationships

- Monitoring Needed at all levels
  - Account Providers
  - Party Entrance
  - Federations
- Performance as good (or bad) as members

Bootstrap: Incentives

- Why should I be a user
  - Pseudonym account gets me past annoyances of fully anonymous accounts:
    - spam filters, CAPTCHAs, waiting periods, …
- Why should I be an organizer
  - Pragmatic: Because I'm a service and want to have users
  - Political: Want to support online democracy

Operating Costs

- Short term
  - Scales with user interest
  - More users encourages more services
- Long term
  - Cost should be similar to elections, but for a more general utility
  - Democratic societies accept these costs as worthwhile

Discussion

- “Pseudonym parties may be the worst way of distributing access to online sites and services, except for all the others that have been tried”

--Anonymous Reviewer, with apologies to Churchill

Related Work

- Unreplaceable Pseudynyms [Friedman & Resnick]
- PGP key signing parties
- SybilGuard, SybilLimit [Yu, Kaminsky, Gibbons, Xiao]
- Sybil DHT [Lesniewski-Laas]

List of Questions

- What if I miss this year's party?
- What happens when my pseudonym account server breaks or shuts down?
- What if my account is stolen?
- Can {rich evil person} get a pile of identities by paying people to attend?

Summary

- Accountable pseudonyms
- One person, one persona per service
- Maintain privacy
- Implementation Sketch: Pseudonym Parties
  - Operation & costs similar to elections
  - Grown organically
  - Usable for many services