Bringing P2P to the Web: Security and Privacy in the Firecoral Network

Jeff Terrace

Sean Stern

Harold Laidlaw

PRINCETON UNIVERSITY

Hao Eric Liu

Michael Freedman

Slashdot Effect

Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://box4.mercumaya.net/suspended.page/

Slashdot - Main Stories (20)   http://box4.m...pended.page/

This Account Has Been Suspended

Please contact the billing/support department as soon as possible.

Views (red) / Downloads (blue)

Internal Server Error

The server encountered an internal error or misconfiguration and was unable

Please contact the server administrator, support@supportwebsite.com and in

More information about this error may be available in the server error log.

*Apache/1.3.33 Server at www.gocfr.com Port 80*

Network Timeout

The server at rickmahn.com is taking too long to respond.

The requested site did not respond to a connection request and the browser has stopped waiting for a reply.

- Could the server be experiencing high demand or a temporary outage? Try again later.
- Are you unable to browse other sites? Check the computer's network connection.
- Is your computer or network protected by a firewall or proxy? Incorrect settings can interfere with Web browsing.
- Still having trouble? Consult your network administrator or Internet provider for assistance.

Try Again
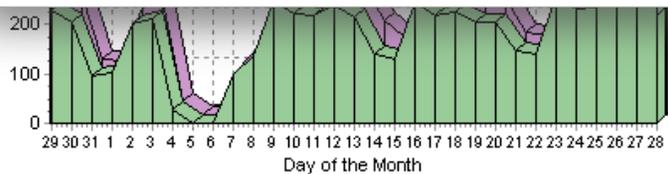
Untitled - Galeon

File Edit View Tab Settings Go Bookmarks Tools Help

Back   Forward   Reload   Home   Stop   100   http://www.armadill

Google » Google » Google GROUPS » Google IMAGES « »

Search Daily BLOGs Weekly Linux TV Guide SpellCheck

Too many users... blah blah blah

Probable cause: http://www.slashdot.org

Try again in a few seconds...

-xian@idsoftware.com

Done.

2,600 2,400 2,200 2,000 1,800 1,600 1,400 1,200 1,000 800 600 400 200 0

200 100 0

29 30 31 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
Day of the Month

Existing Commerical CDNs

- Build your own solution
  - Expensive to set up
  - Only cost effective at massive scale

- Purchase from provider
  - Expensive
  - Requires prior knowledge of demand

Existing Free CDNs

- ## Peer-to-peer CDNs
  - Easy to use
  - Free!
  - Automatic redirection

- ## Unfortunately...
  - Over-subscribed
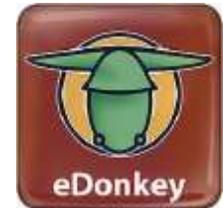 - Under-provisioned
  - Scalability limited due to trust

Existing P2P Networks

- ## Leverage file-sharing networks
  - Demonstrated to provide scalability, fairness, and high-performance

- ## Design Mismatch
  - Not easily integrated into web browsers
  - High latency cost for small files

Introducing Firecoral

- **What is Firecoral?**
  - A peer-to-peer network for the web
  - Integrates directly into a user's web browser
  - Ensures authenticity of content
  - Preserves user privacy
  - Backwards compatible

- **This talk's focus**
  - Security
  - Privacy
  - Usability

- **Not focused on**
  - P2P Algorithms
  - Incentives
  - Evaluation

Firecoral Goals

- ## Content Providers
  - Easily integrate into existing web servers
  - Backwards compatibility
  - Not interfere with advertisements and analytics

- ## End Users
  - Easy to install and transparent to use
  - Provide content integrity
  - Respect privacy/sharing policies

Modified Content Provider

- Content Provider
  - Acts as tracker
  - Ensures authenticity

Content Provider

<URL>

<Content Hash>
<Peer List>

Client

Peer

URL

Peer

URL

URL

Peer
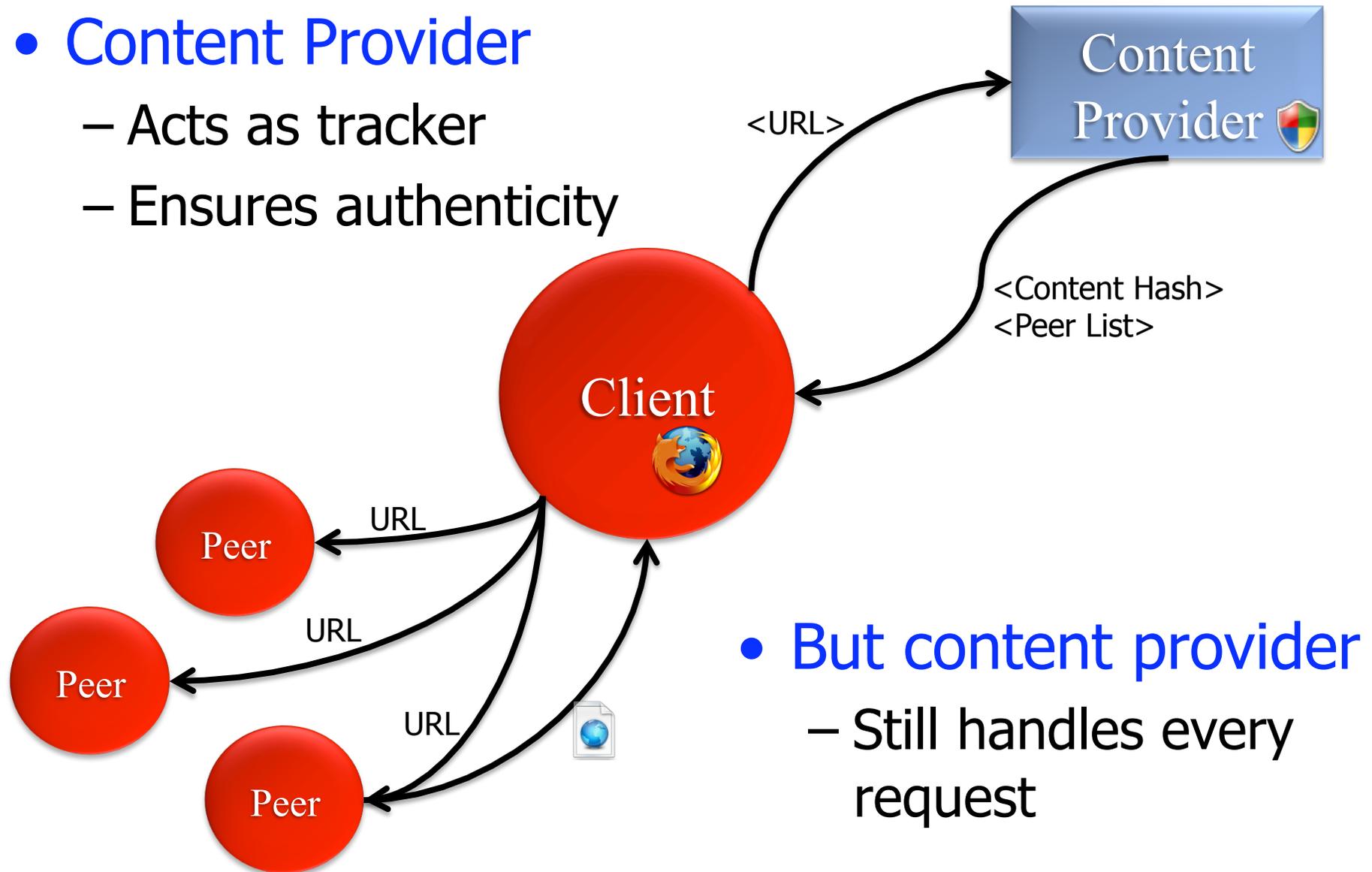
- But content provider
  - Still handles every request

External Tracker
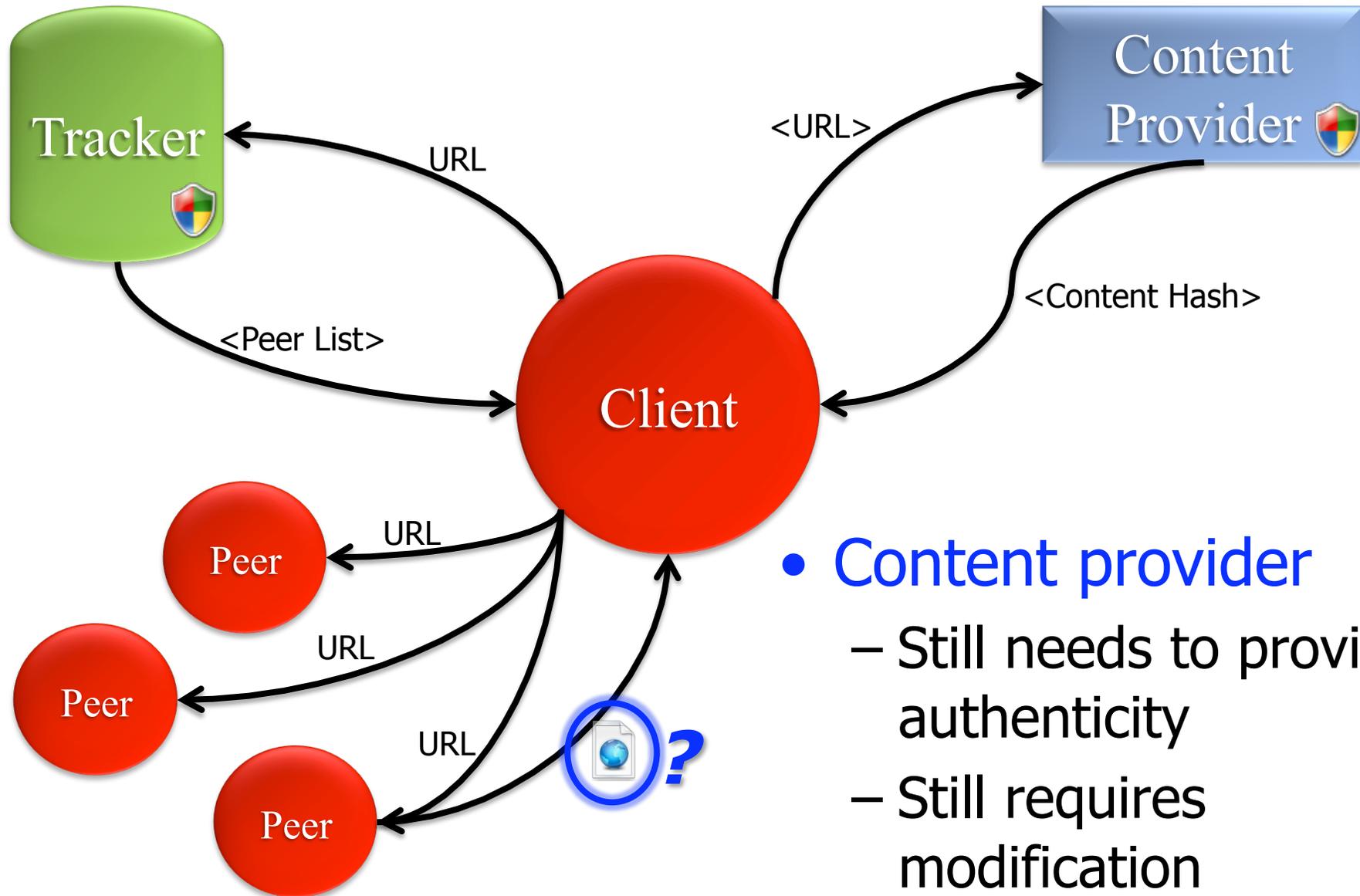
- Content provider
  - Still needs to provide authenticity
  - Still requires modification

Signing Service

Tracker

Client

Peer

Peer

Peer

Content Provider

Signing Service

URL

Sig$_{SS}$<Content Hash>
<Peer List>

URL

URL

URL

URL

URL

Private Key = SS
Computes
Sig$_{SS}$<Content Hash>

When to Use Firecoral
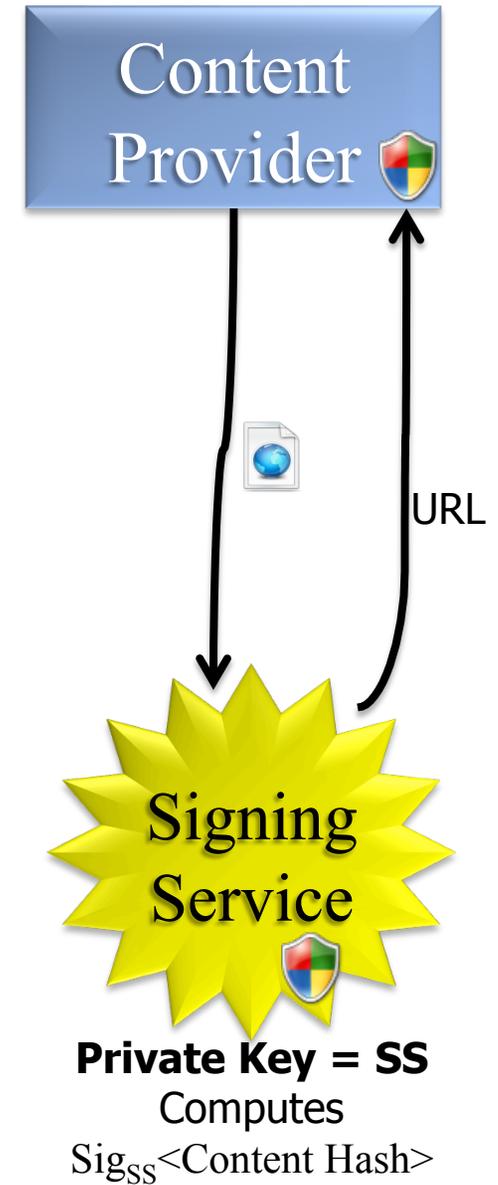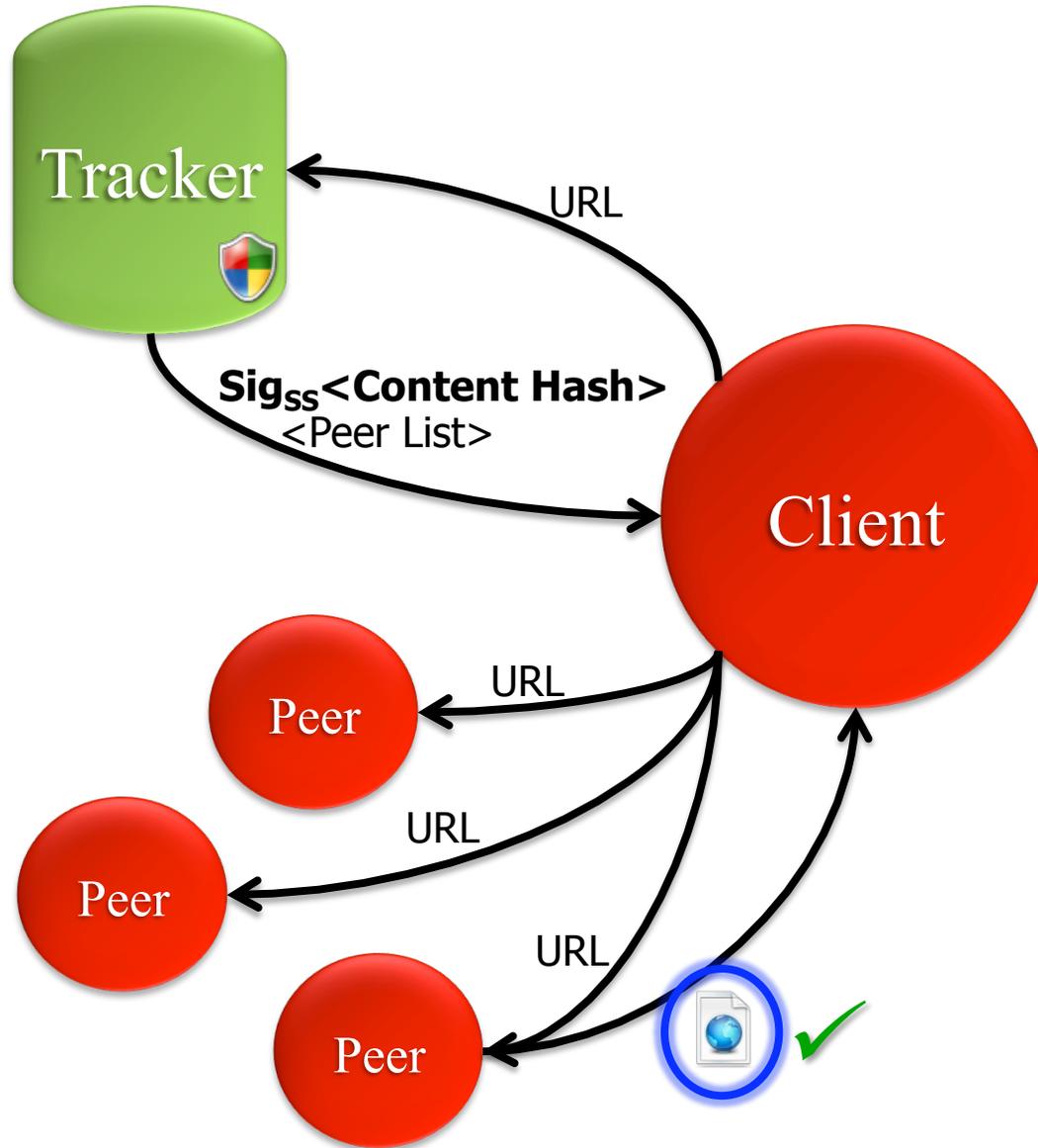
- ## Content to avoid
  - ### HTTPS
    - Banking
    - Online Shopping

  - ### POST Requests
    - Web mail
    - Feedback forms

  - ### Other private content?

When to Use Firecoral

- ## Simply list domains
  - Too coarse grained
  - Requires site lists be known

- ## Use HTTP referrer header
  - Captures 3rd party advertisements
  - Interferes with analytics

Configuration Example

Configuration Solution

- ## HTML Text
  - Difficult to parse
  - Requires maintenance

- ## Web standards!
  - XML Path Language (XPath)
  - Queries can select XML nodes from HTML
  - XPath rules are simple and easy to write
  - Firefox executes XPath very quickly

XPath Example

- Query for digg.com used to be:

  //div[@class='news-summary']
  /descendant::a[starts-with(@href, 'http://')
  and not(contains(@class, 'thumb'))]/@href

- Digg releases "DiggBar" feature which changes HTML

- New query only changes one word:

  //div[@class='news-summary']
  /descendant::a[starts-with(@href, 'http://')
  and not(contains(@class, 'thumb'))]/@**title**

Subscriptions

- **List of Domain/XPath pairs**

- **Whitelist**
  - Use Firecoral
  - Contains popular news aggregators

- **Blacklist**
  - Don't use Firecoral
  - Contains known well-provisioned sites

Implementation

- ## Tracker
  - 1000 lines of PHP running on Apache
  - Uses MySQL, Memcachedb, and Memcached

- ## Signing Service
  - 700 lines of Python

- ## Firefox Extension
  - 7000 lines of JavaScript, XUL, and CSS
  - Runs an HTTP proxy server within Firefox
  - Uses Mozilla XPConnect API for access to low-level network functions
  - Cross platform

Demo

Conclusions

- Firecoral brings P2P to the web
- Firecoral provides
  - Security
  - Privacy
  - Usability
- Allows content providers to easily support Firecoral
- Allows users to easily configure sharing and privacy policy

Future Work

- ## Implementation
  - NAT traversal
  - Apache plug-in for signing and redirection

- ## Design
  - Incentives
  - Peer selection
  - Measurement study

Thank You

Questions?

http://firecoral.net/