

# Hiding in Public: File Management in Unsafe Conditions

Abram Hindle, Andrew Wong

<http://churchturing.org>

[abram.hindle@softwareprocess.us](mailto:abram.hindle@softwareprocess.us)

February 27, 2008

# Introduction

- File Store
- Unsafe/Untrusted server
- Limit to Trusted Clients
- Cannot store keys on Server
- Require only default perl and OpenSSL

# Server

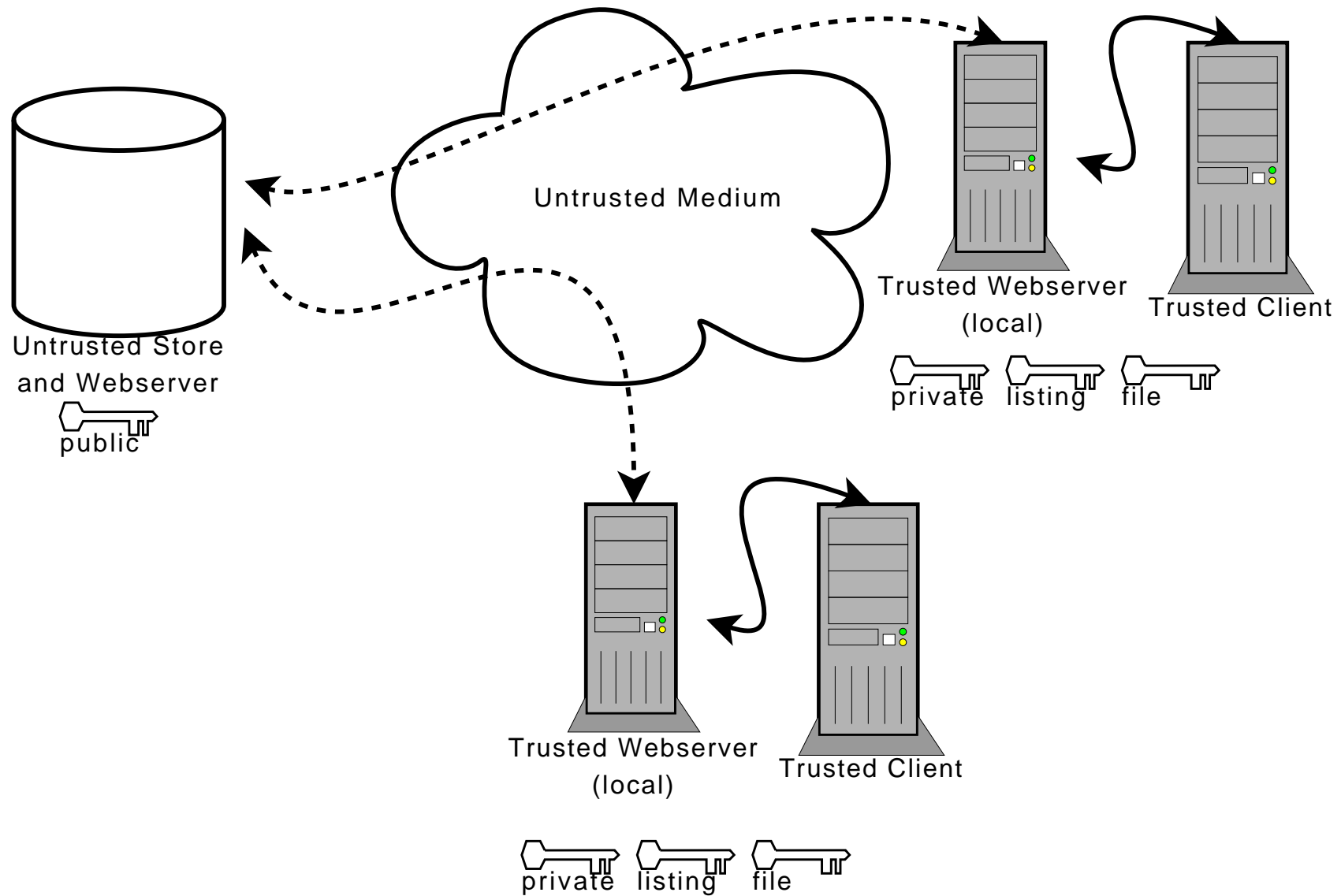
- We don't trust the host.
- We don't want the host to have any knowledge of the files being store
  - Although size and directory structure is ok
  - Didn't want to have develop a new file format
  - Wanted to take advantage of static content serving

# Client

- Easy to upload
- Easy to download via a proxy
  - Proxy does name translation
  - Proxy does decryption on the fly



20:56	<a href="#">_darcs</a>
20:56	<a href="#">server.scm</a>
20:56	<a href="#">model.scm</a>
20:56	<a href="#">opengl-utilities.scm</a>
20:56	<a href="#">client.scm</a>
20:56	<a href="#">utilities.scm</a>



# Crypto

- Levels of access: None, Browsing, Download, Upload, Upload and Download
  - Download - file symmetric key
  - Upload - RSA key for signing uploads
  - Browsing - Symmetric Key
- OpenSSL used for all crypto, symmetric and public key
- Everything sent over untrusted links

# Perl

- Uploader script uses LWP
- Proxy Script is a CGI which uses LWP's call-back  
: `content_cb` to pipe into `openssl`
- Around 600 lines of perl
  - Server side: directory lister and file upload/verifier
  - Client side: Proxy and Uploader

# Bugs

- Currently weak to replay attacks (you can do the same upload)
- Some UTF8 filename encoding problems (help!)
- Maybe some path escaping bugs? Used File::Spec

# Conclusions

- Installable in most environments by default
- Relatively safe, encrypted shared file repository
- Doesn't consume much resources on the server side
- Email me [abram.hindle@softwareprocess.us](mailto:abram.hindle@softwareprocess.us) or visit
  - <http://churchturing.org/>

# Directory Tree Example

- ```
.
|-- 2E+jz3bTo2kIUIG7AZwUUQ==
|  `-- 1+0+sH4J0so=
|     |-- 28CaLj0RO_AIY4CNjNP3qw==
|     |-- c_zmRIFtpK2fenoF7HrqoQ==
|     `-- sBIkeihZwys=
|-- 6TD4MS7r7zE=
|     |-- 0aL8x5Am+cxMRMv6LtaCsjWaviSOM+V76
|     |-- 0jr5+c4HQfPpFxt8hk_DpFezG0_NOGma
```