Cloud Storage Security

Sven Vowé

Fraunhofer Institute for Secure Information Technology (SIT)

Darmstadt, Germany

SIT is a member of CASED (Center for Advanced Security Research Darmstadt)

CASED

Fraunhofer
SIT

Cloud Storage Security
Outline

1. **Introduction and overview**
2. Features
3. Security requirements
4. Security issues
5. Trust issues
6. Drawbacks
7. Choice

Introduction: Basic Cloud Storage Services

- Simple online data storage
  - Independent of physical location
  - Provides rudimentary REST API
  - Several mature service providers
  - Very low costs
    - pay-per-use model
- Use-Cases
  - data sink for (online) applications
  - data sink for virtual machines
  - online backup for arbitrary data
  - online access to arbitrary data

Example: Amazon S3 Pricing (August 2012)	
Standard Storage (up to 1TB)	Each GB = $0.125
PUT, COPY, POST, LIST	1,000 Requests = $0.01
GET	10,000 Requests = $0.01
Transfer IN	$0
Transfer OUT (up to 10TB)	Each GB = $0.12
Example: 100GB, 10.000 Files, one Month	
Initial Upload	$0.10
Storage	$12.50
Download	$12.01
Total	**$24.61**

Introduction: Basic Cloud Storage Services

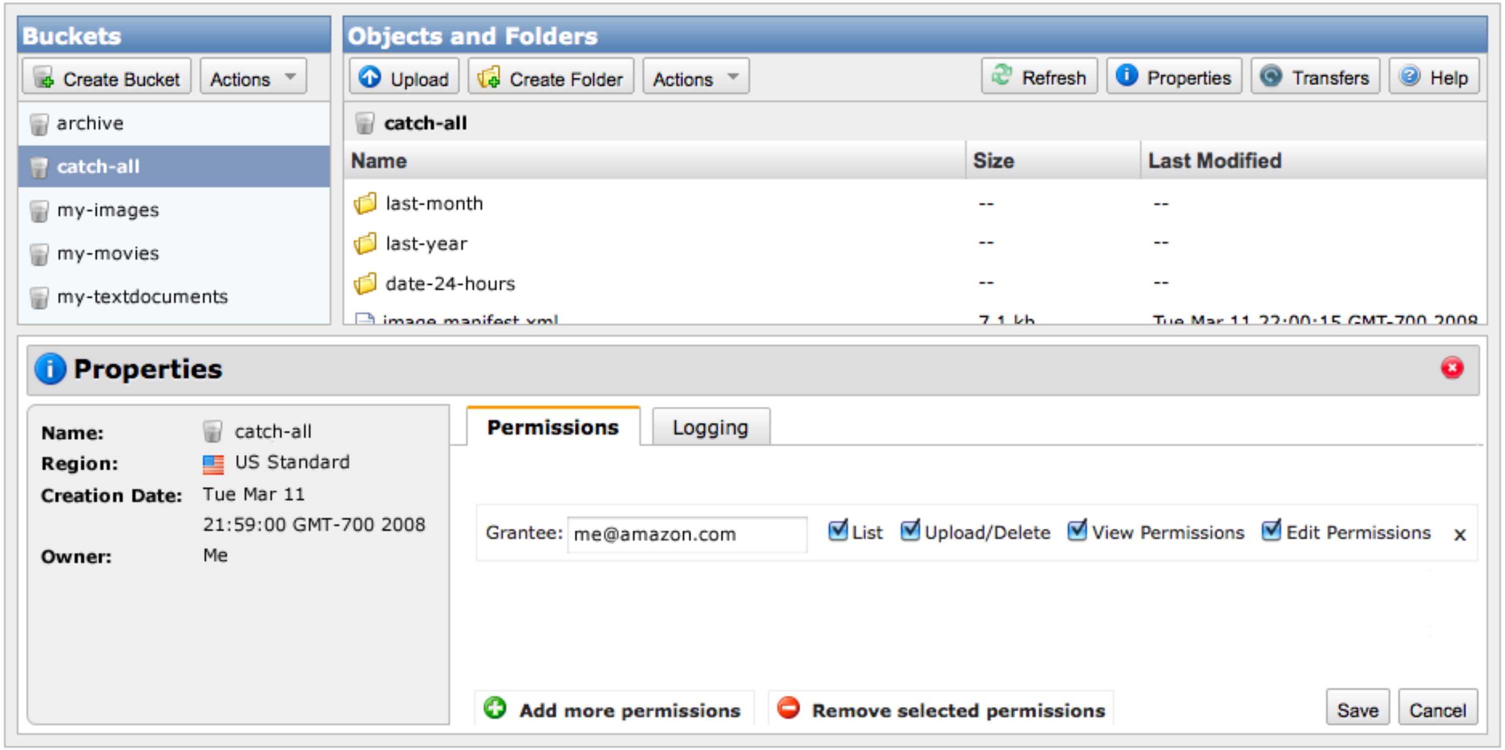
- Service includes
  - Multiple redundancy
  - 99.99999% availability
  - REST / Browser interfaces
- Vs. data center operational costs
  - Physical location
  - Staff
  - Power consumption
  - Uplink
  - Bandwidth
  - etc...

Example: Amazon S3 Pricing (August 2012)	
Storage <= 1TB	Each GB = $0.125
Storage 1TB … 50TB	Each GB = $0.110
Storage 50TB … 500TB	Each GB = $0.095
PUT, COPY, POST, LIST	1,000 Requests = $0.01
GET	10,000 Requests = $0.01
IN	$0
OUT <= 10TB	Each GB = $0.12
OUT 10TB … 50TB	Each GB = $0.09

Example: 100TB, 1,000,000 Files, one Month	
Initial Upload	$10.00
Storage	$10,511.36
Download	$4916.20
Total	**$15,437.56**

Introduction: Basic Cloud Storage Services

- Why doesn't everybody use it?
  - Costs/Data ratio scaled to massive data amounts
  - Cumbersome data handling
  - End-User clearly not targeted



- archive
- catch-all
- my-images
- my-movies
- my-textdocuments

catch-all

Name	Size	Last Modified
last-month	--	--
last-year	--	--
date-24-hours	--	--
image manifest.xml	7.1 kb	Tue Mar 11 22:00:15 GMT-700 2008

Name: catch-all
Region: US Standard
Creation Date: Tue Mar 11 21:59:00 GMT-700 2008
Owner: Me

Grantee: me@amazon.com ☑ List ☑ Upload/Delete ☑ View Permissions ☑ Edit Permissions x

Introduction: Advanced Cloud Storage Services

- Simple online data storage
  - independent of physical location
  - Very easy to use
  - Several plans with fixed costs
  - Many providers
- Great demand
  - Summer 2011: Dropbox reached 25 Million users
- Use-Cases
  - data backup, synchronization, transfer, accessibility
  - mobile data access, co-operation

CloudMe
CRASHPLAN™
Dropbox
mozy
TeamDrive
Sync your data fast & secure
ubuntu one
wuala by LACIE

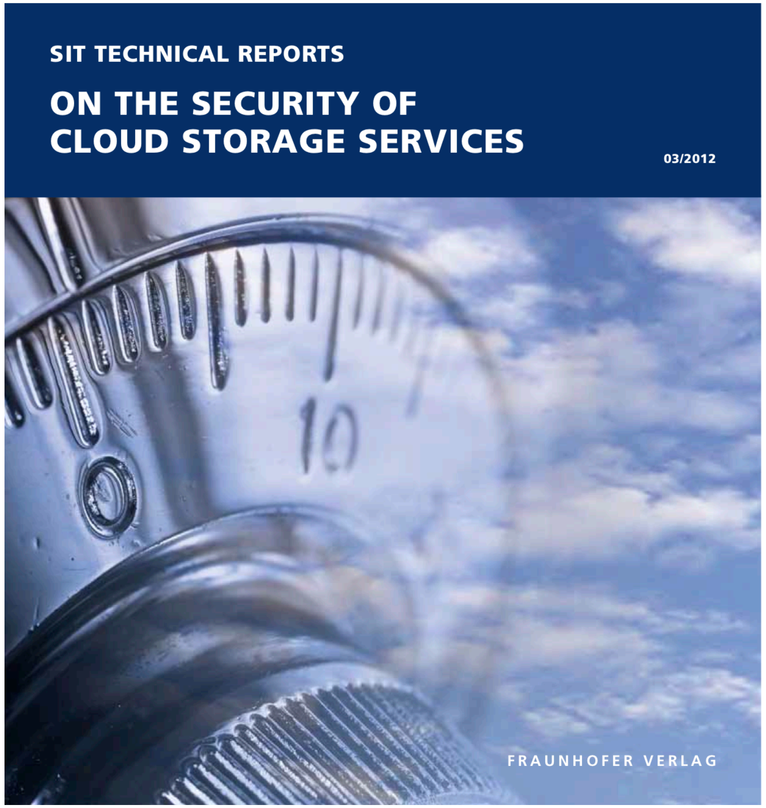
Introduction: Advanced Cloud Storage Services

- Payment models
  - Basic variant free
    - Provides a bit of space
  - Expanded variants with monthly costs
    - More storage space
    - Multiple user functionality
      - i.e. Team collaboration
    - Professional Support
      - i.e. Telephone
    - Tool Support
      - i.e. ActiveDirectory

Example: Dropbox Pricing (August 2012)	
FREE: 2GB Storage	$0
PRO: 100GB	$9.99 / month
PRO: 200GB	$19.99 / month
PRO: 500GB	$49.99 / month
TEAM: 1000GB (5 Users)	$795.00 / year
PRO 200: 200GB / account (5 users)	$995.00 / year

Interlude: Technical Report by Fraunhofer SIT

- 2011
  - Analysis of several Advanced Cloud Storage Services
    - Functionality
    - Security
- 2012
  - Published Study / Technical Report “On the Security of Cloud Storage Services”
    - freely available



SIT TECHNICAL REPORTS

ON THE SECURITY OF CLOUD STORAGE SERVICES

03/2012

FRAUNHOFER VERLAG

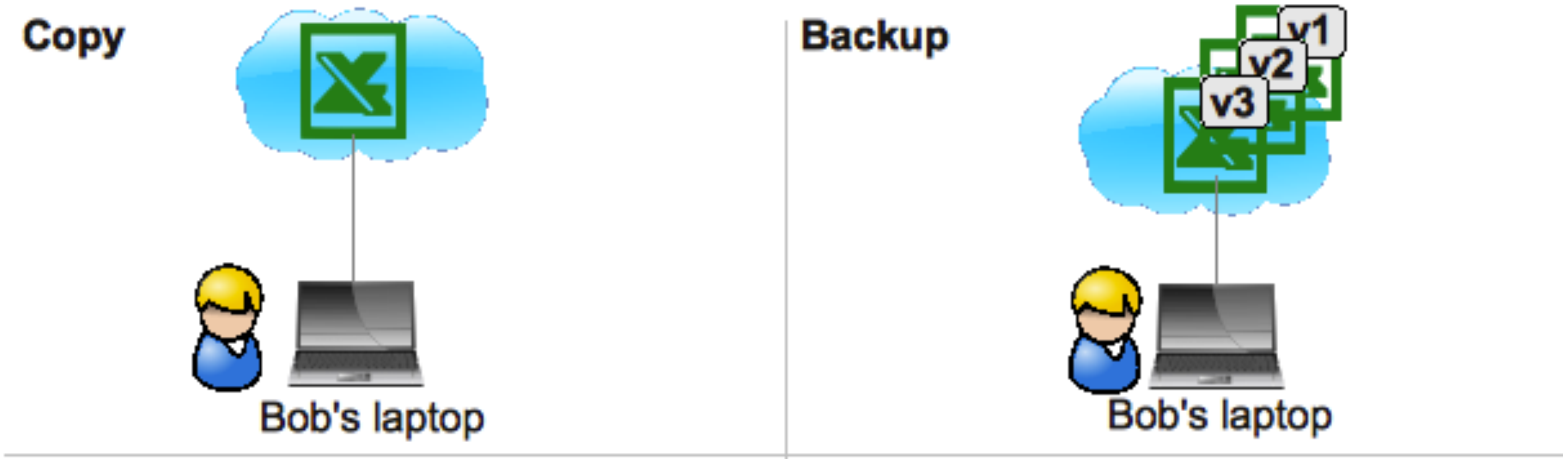
Download here: http://www.sit.fraunhofer.de/en/cloudstudy.html

Cloud Storage Security
Outline

1. Introduction and overview
2. **Features**
3. Security requirements
4. Security issues
5. Trust issues
6. Drawbacks
7. Choice

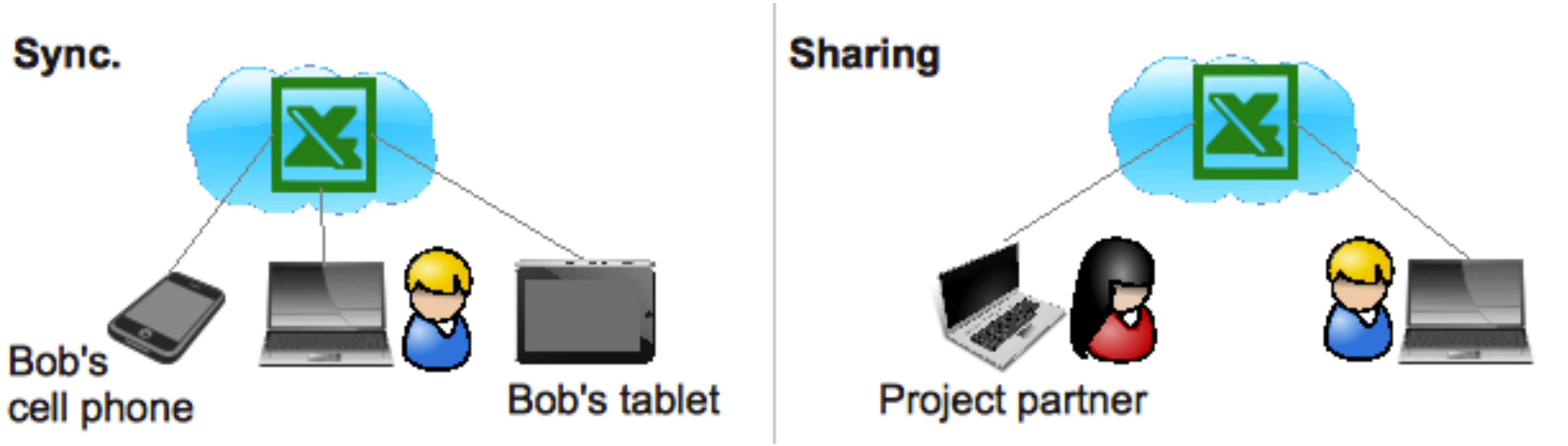
Features for End-Users

- Simple Features
  - Copy files to online storage
  - Backup files to online storage
    - Usually with versioning



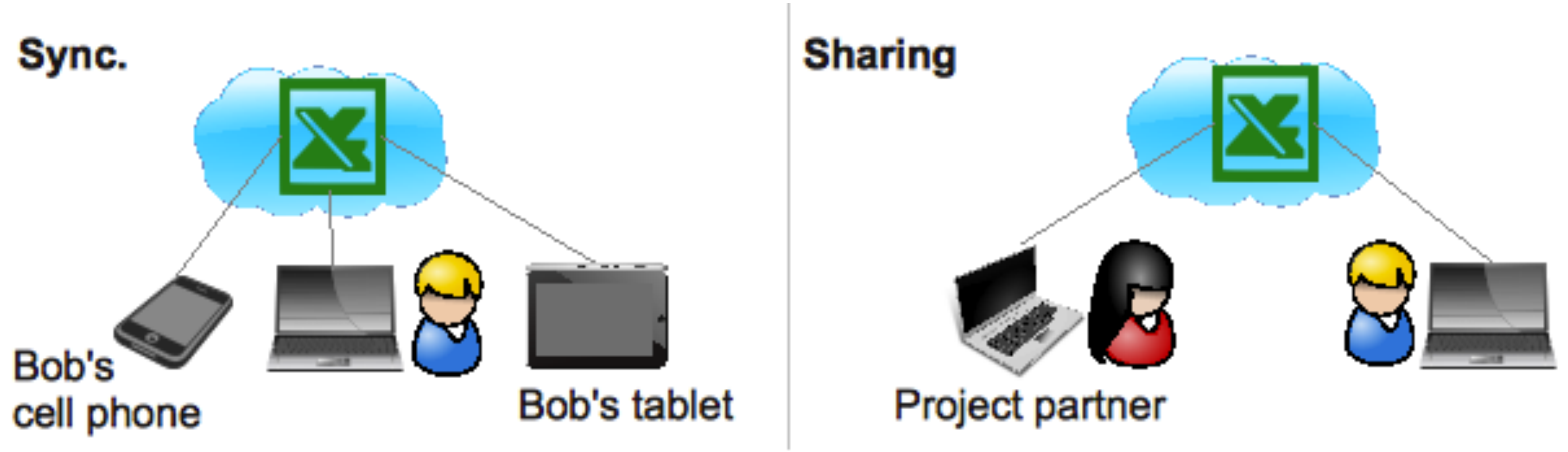
Features for End-Users

- Advanced Features
  - Synchronize files with multiple linked devices
    - Pull synchronization: manual updates (git, subversion work like that)
    - Push synchronization: automatic updates by client software



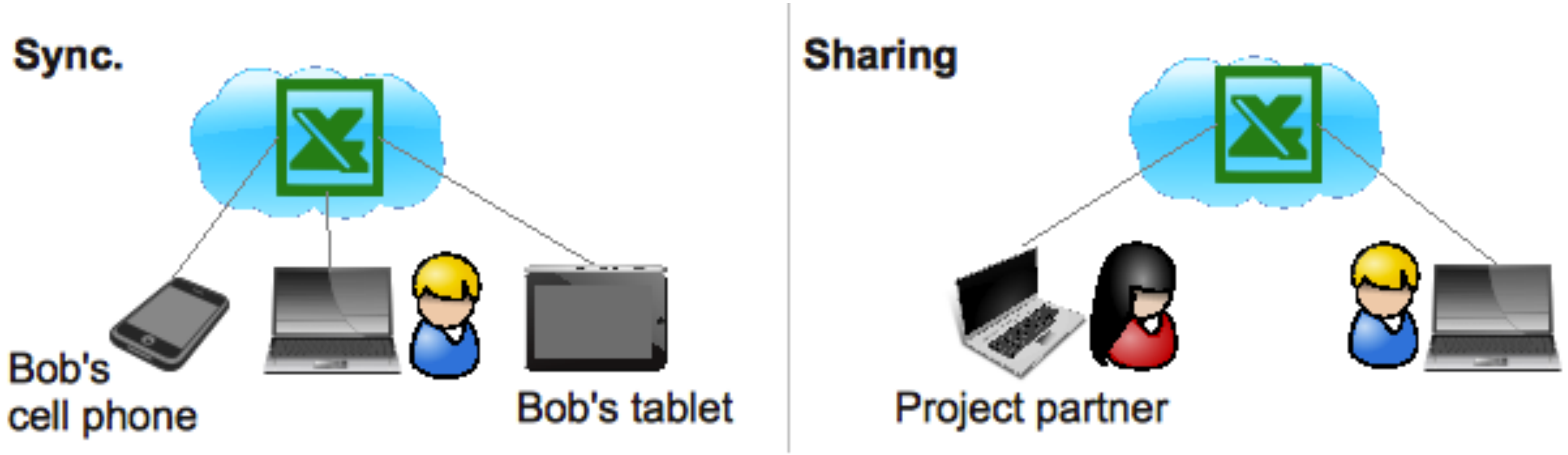
Features for End-Users

- Advanced Features
  - Share data with others
    - Sharing: exchange data with other users of the service
    - Publishing: Generate public URL and distribute to other users



Features for End-Users

- Advanced Features can be combined
  - Push Synchronization and Sharing
    - Cross-User Synchronization
      - Files changed by others automatically downloaded to linked devices



Features for End-Users

- Several Services specialize in subset
- Supported Features

Service	Copy	Backup	Synchronization	Sharing
CloudMe	✓	✗	✗	✓
Crashplan	✗	✓	✗	✗
Dropbox	✓	✗	✓	✓
Mozy	✗	✓	✗	✗
TeamDrive	✓	✓	✓	✓
Ubuntu One	✓	✗	✓	✓
Wuala	✓	✓	✓	✓

Features: Deduplication

- Service providers pay traffic and storage
- Many use internal minimization technique: Deduplication
  - Server-side deduplication
    - incoming file already exists → only save link
  - Client-side deduplication
    - Client sends file information to server
    - File already exists → do not upload, only save link
- Providers claim storage reduction of **70% - 90% !!!**

Cloud Storage Security
Outline

1. Introduction and overview
2. Features
3. **Security requirements**
4. Security issues
5. Trust issues
6. Drawbacks
7. Choice

Security Requirements

- Registration and Login
  - Strong passwords
  - Protection against username/email enumeration
- Transport
  - Server authentication & Hostname Verification
  - Suitable cryptography
- Encryption
  - Client-side encryption of data and filenames
  - Non-deterministic key generation
  - Suitable cryptography

Security Requirements

- File sharing
  - Obfuscated public URLs
  - No indexing by external search engines
  - Reversible sharing
  - Disinvited users excluded by cryptographic means
- Deduplication
  - Deduplication threshold OR
  - single-account deduplication

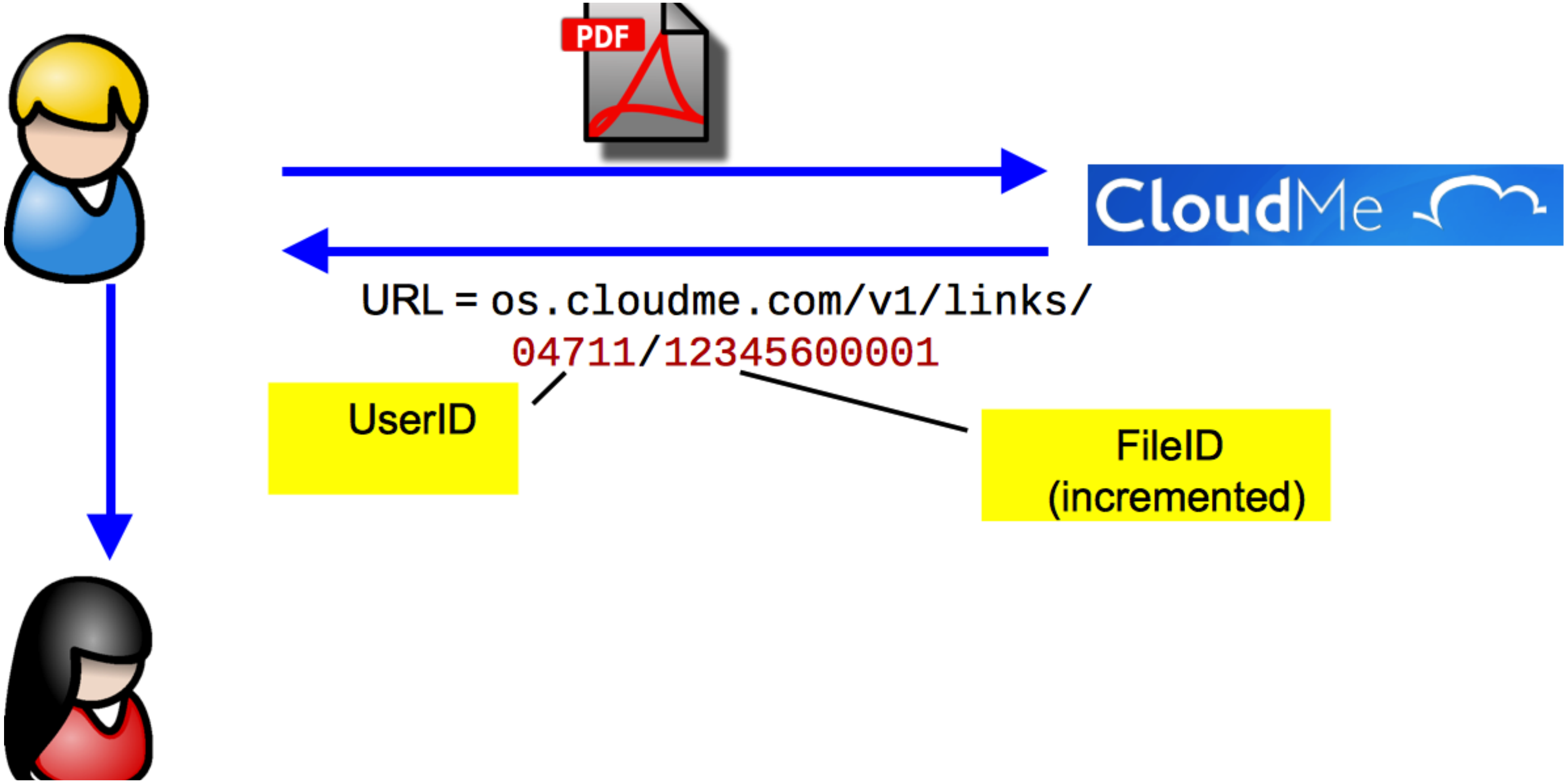
Security Requirements

- Synchronization
  - List of registered devices
  - Manual device activation
  - Manual device deactivation
- Client software updates
  - Integrated periodic update check
  - User-initiated or silent update
- Server location
  - Storage location information

Cloud Storage Security
Outline

1. Introduction and overview
2. Features
3. Security requirements
4. **Security issues**
5. Trust issues
6. Drawbacks
7. Choice

Security Issues: Careless Publication



URL = `os.cloudme.com/v1/links/`
`04711/12345600001`

UserID

FileID
(incremented)

Security Issues: Careless Publication

- Allows download of all public files
  - Iterate through UserID
    - Iterate through FileID

- Some allowed search engine indexation
  - Public files found by URL-based search
  - File contents indexed
    - Eases search for sensitive data

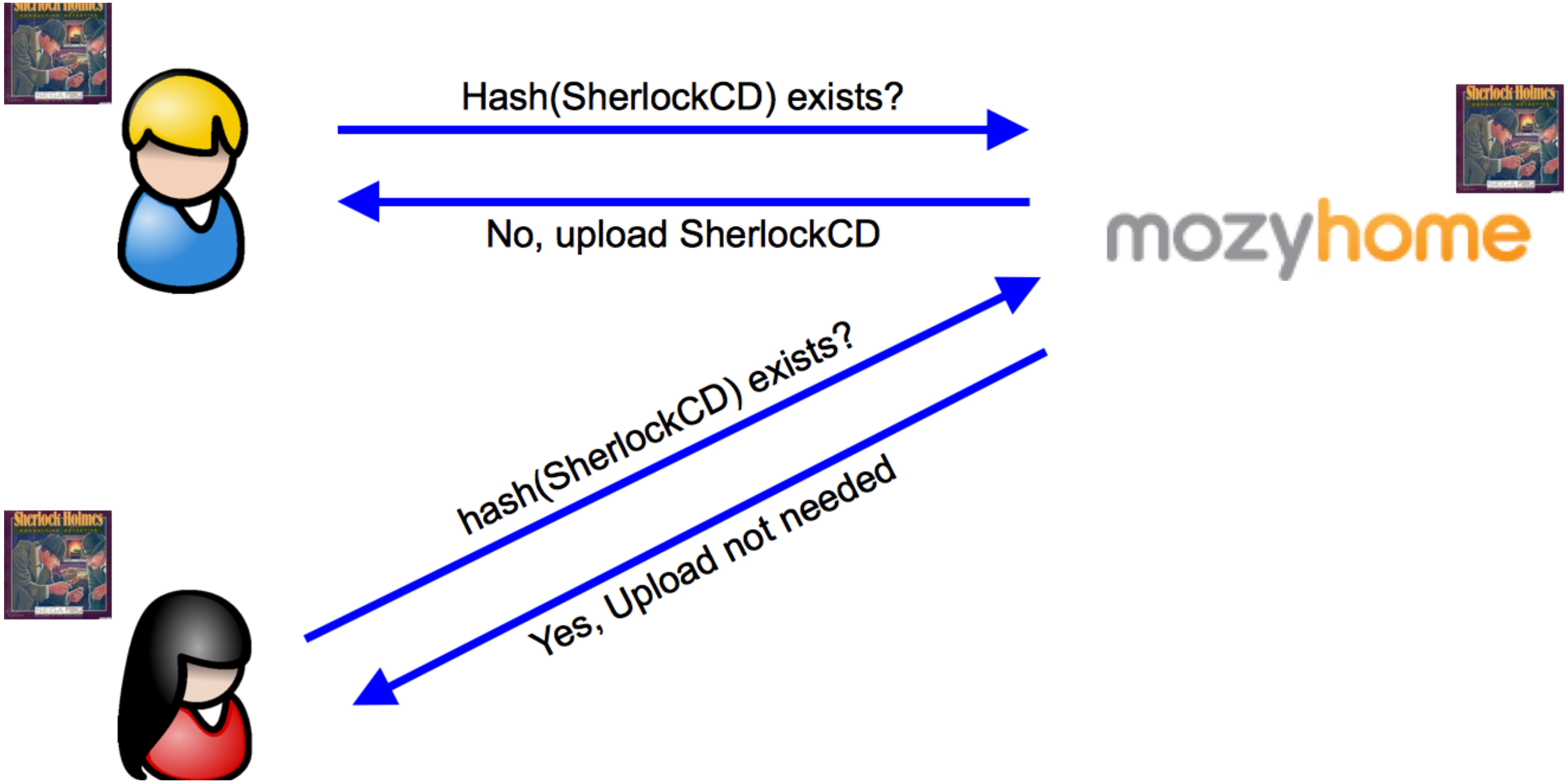
Security Issues: Careless Publication

- Mitigation Strategies
  - Use obfuscated URL
    - http://serviceprovider.com/public/<HASH(RANDOM + HASH(FILE))>
  - Disallow search engine indexations
    - I.e. robot.txt:

```
User-agent: *
Disallow: /
```

Security Issues: Deduplication

- Client-side Deduplication



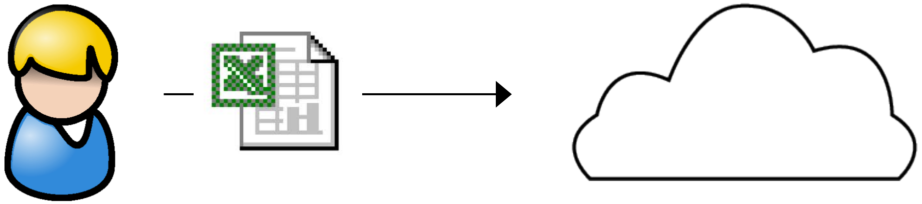
Security Issues: Deduplication

- Benny Pinkas, 2010: Client-side Deduplication
  - Allows to test for file existence
    - If no upload occurs, document is already there

© Fraunhofer-Gesellschaft 2012

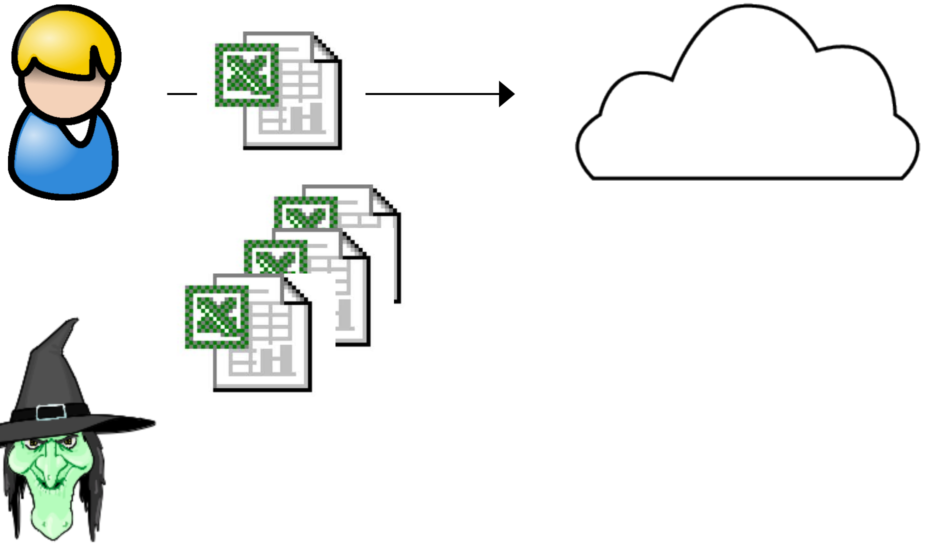
Security Issues: Deduplication

- Benny Pinkas, 2010: Client-side Deduplication
  - Allows espionage attack
    1. Bob uploads salary sheet



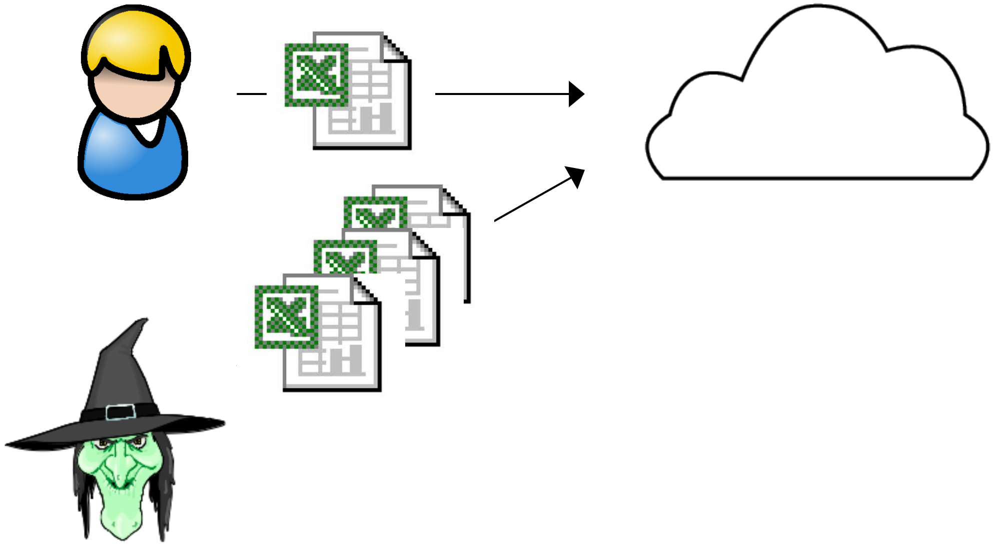
Security Issues: Deduplication

- Benny Pinkas, 2010: Client-side Deduplication
  - Allows espionage attack
    1. Bob uploads salary sheet
    2. Attacker knows document outline and creates possible documents



Security Issues: Deduplication

- Benny Pinkas, 2010: Client-side Deduplication
  - Allows espionage attack
    1. Bob uploads salary sheet
    2. Attacker knows document outline
    3. Attacker uploads possible salaries until no upload occurs



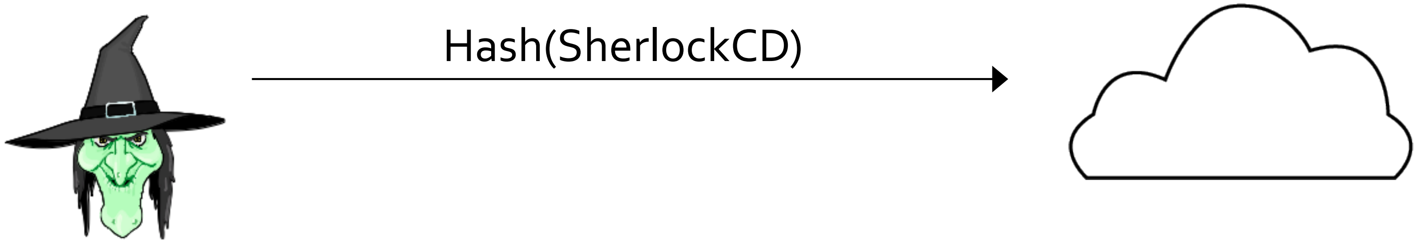
Security Issues: Deduplication

- Benny Pinkas, 2010: Client-side Deduplication
  - Allows document takeover
    1. Attacker knows the hash of a file

Hash(SherlockCD)

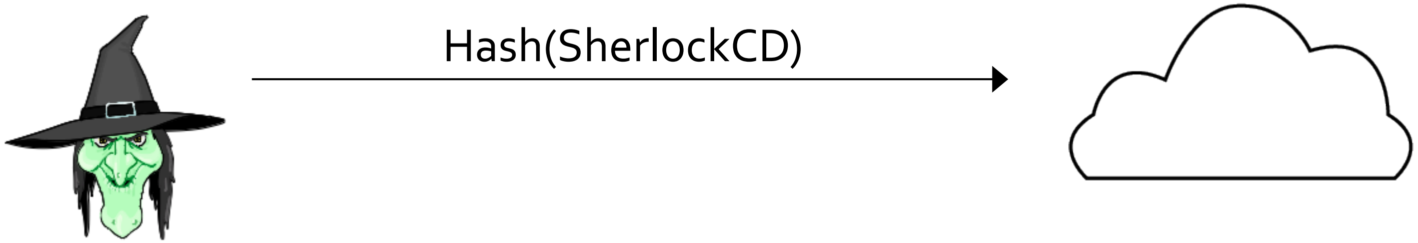
Security Issues: Deduplication

- Benny Pinkas, 2010: Client-side Deduplication
  - Allows document takeover
    1. Attacker knows the hash of a file
    2. Attacker manipulates communication to server and injects hash



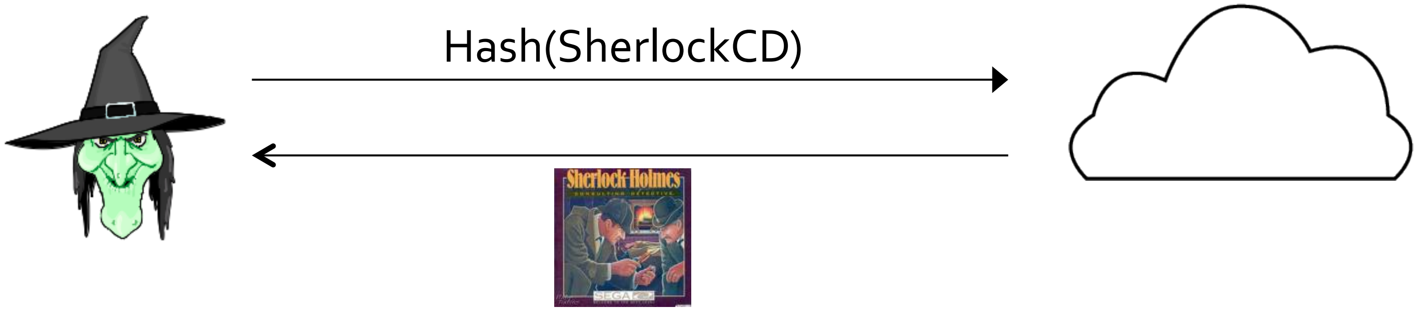
Security Issues: Deduplication

- Benny Pinkas, 2010: Client-side Deduplication
  - Allows document takeover
    1. Attacker knows the hash of a file
    2. Attacker manipulates communication to server and injects hash
    3. Server sets a link to the file, registers attacker as owner



Security Issues: Deduplication

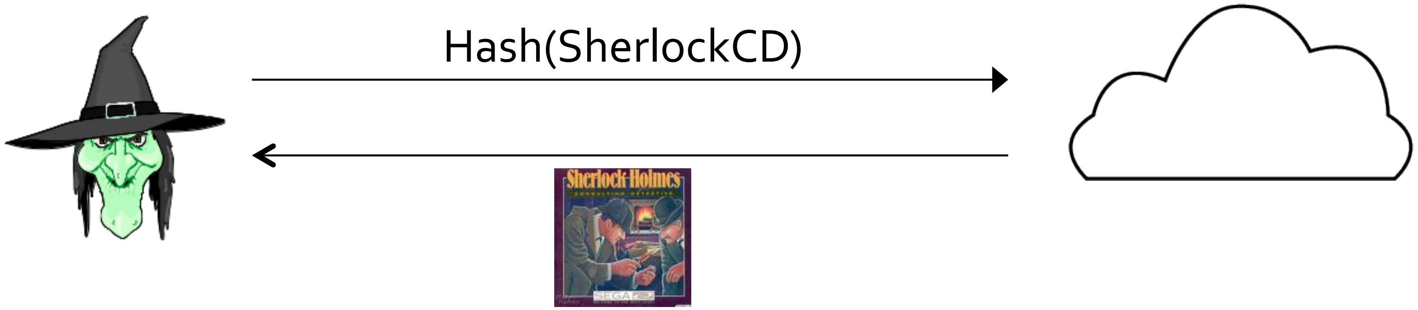
- Benny Pinkas, 2010: Client-side Deduplication
  - Allows document takeover
    1. Attacker knows the hash of a file
    2. Attacker manipulates communication to server and injects hash
    3. Server sets a link to the file, registers attacker as owner
    4. Attacker downloads file



Security Issues: Deduplication

- Client-side Deduplication
  - 2011: Dropship (https://github.com/driverdan/dropship)
    - Open source software exploited the flaw in Dropbox
    - Insertion of hash → File appears in Dropbox folder
    - Dropbox tried to shut down the project
    - Finally, Dropbox disabled client-side deduplication

→ No Cloud Storage Service use Client-Side Deduplication today!



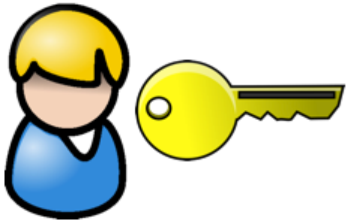
Hash(SherlockCD)

Security Issues: Encryption

- Server-side encryption
  - Data encrypted after transmission
  - No protection against internal attacker at provider
  - No protection against US PATRIOT Act

Security Issues: Encryption

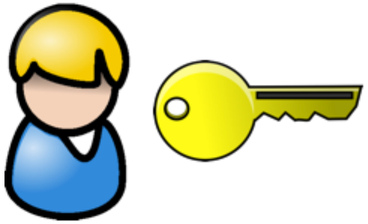
- Server-side key management
  - Client encrypts data before transmission
  - Key is transferred
  - No protection against internal attacker at provider
  - No protection against US PATRIOT Act



  - (Note: Mozy does also allow client to manage key)

Security Issues: Encryption

- Client-side encryption
  - Client generates key
  - Client encrypts data before transmission
  - Protection against external access



TeamDrive
Sync your data fast & secure

Security Issues: Encryption

- Why not always client-side encryption?
  - Lost key = no data access !
  - Not all data needs encryption ?!?

- **Client-side encryption vs. Deduplication !**
  - Copies not detectable
- **Client-side encryption vs. Sharing and Publication !**
  - Additional key exchange methods needed
- **Client-side encryption vs. Usability !**
  - Browser access difficult
  - Synchronization difficult

Security Issues: Wuala‘s convergent encryption

- Wuala employs special method „convergent encryption“

Client

$$\begin{tikzcd}
\text{file} \arrow[r, "\text{hash}"] \arrow[d, "\text{encrypt}"'] & \text{k} \\
\text{enc}_K\text{(file)} \arrow[r, "\text{hash}"] & \text{fname'}
\end{tikzcd}$$

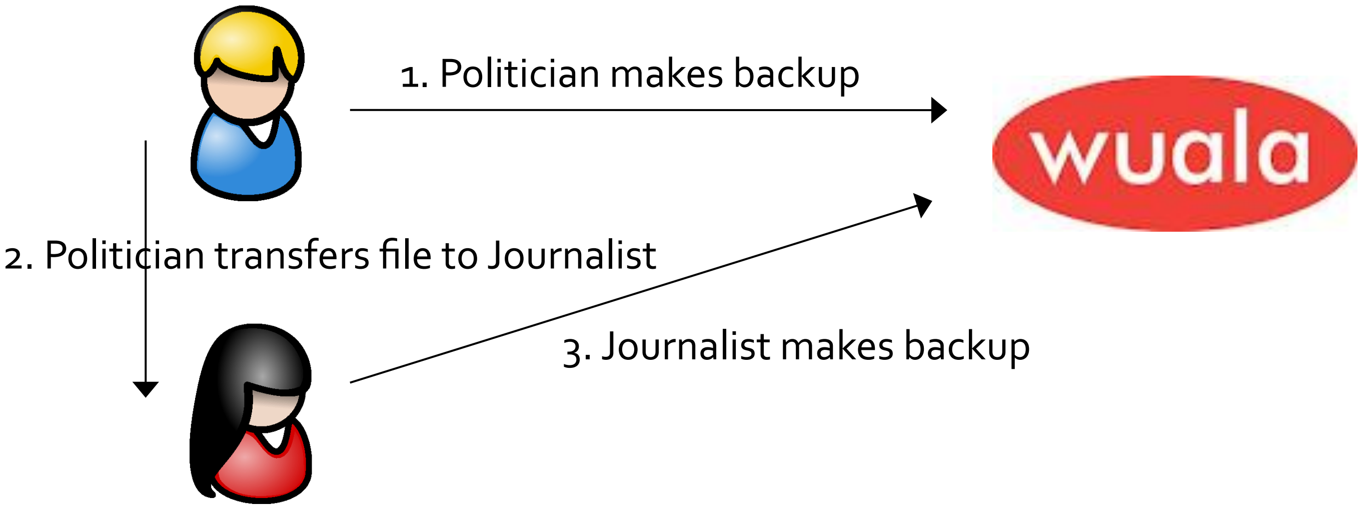
Server

filename on server:	hash(enc$_K$(file))
file content:	enc$_K$(file)
key for decryption:	enc$_S$(k)
filename on user's disk:	enc$_S$(fname)

  - allows use of deduplication
  - allows use of sharing and publication

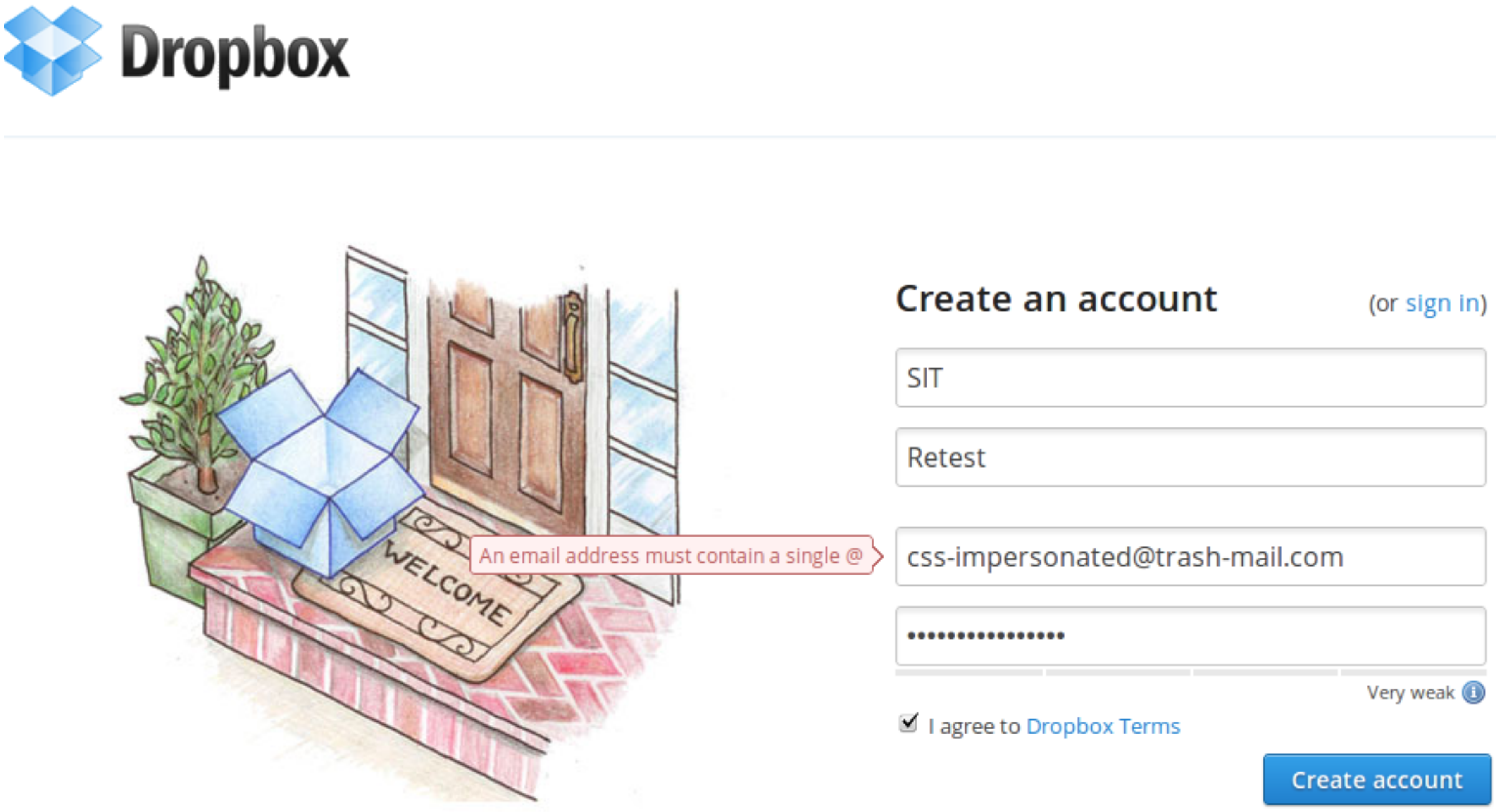
Security Issues: Wuala‘s convergent encryption

- Wuala employs special method „convergent encryption“
  - No protection against internal attacker at provider
  - Example: Leaking a sensitive Document


1. Politician makes backup
2. Politician transfers file to Journalist
3. Journalist makes backup
wuala

Wuala knows:
Politician and
Journalist share
same file

Security Issues: Unverified email addresses



Create an account (or sign in)

SIT

Retest

An email address must contain a single @

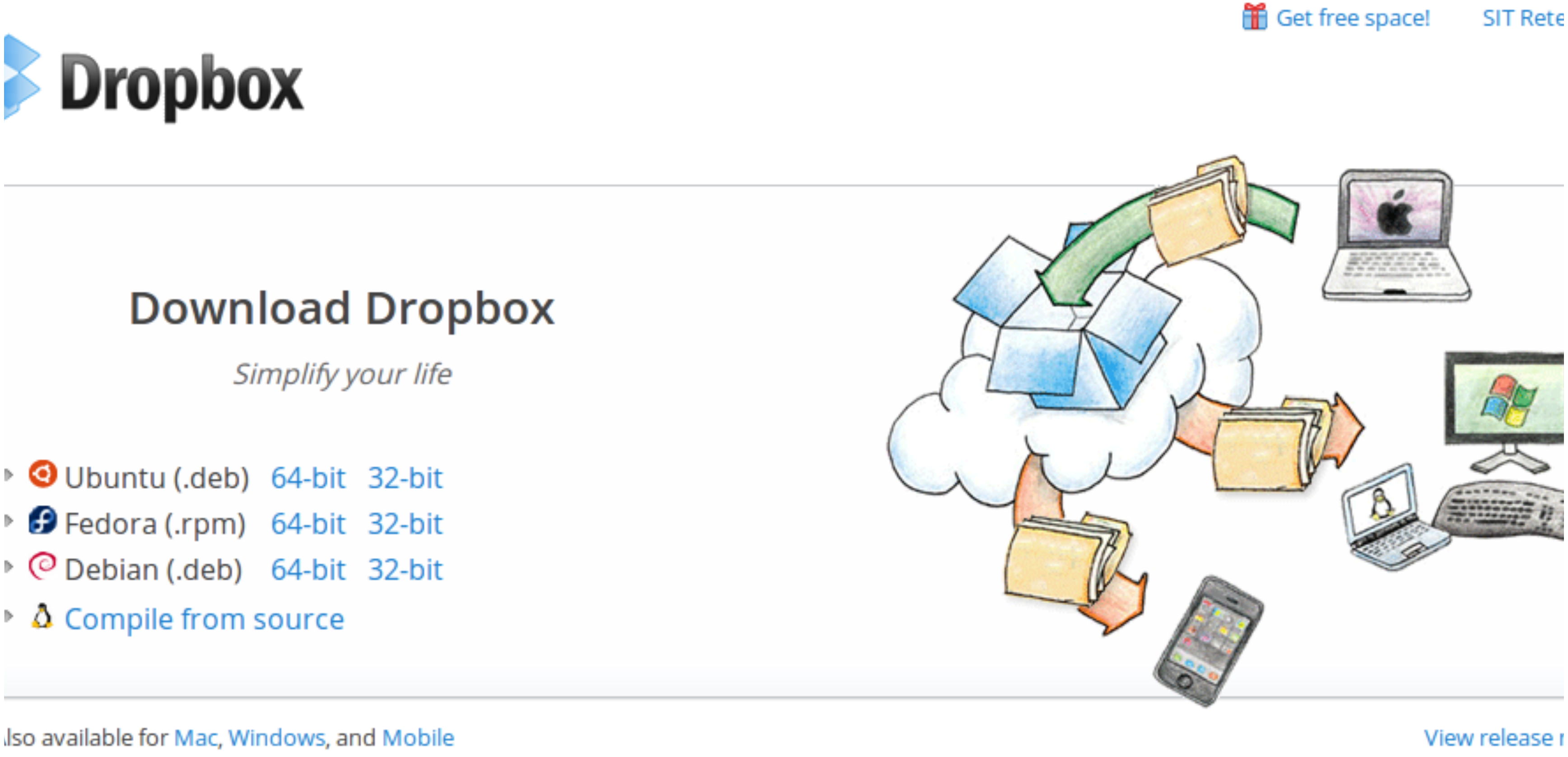
css-impersonated@trash-mail.com

••••••••••••••••

Very weak

☑ I agree to Dropbox Terms

Security Issues: Unverified email addresses



Get free space! SIT Rete

Dropbox

Download Dropbox

Simplify your life

Ubuntu (.deb)	64-bit	32-bit
Fedora (.rpm)	64-bit	32-bit
Debian (.deb)	64-bit	32-bit

- Compile from source

lso available for Mac, Windows, and Mobile

View release r

Security Issues: Unverified email addresses

- Service registration allowed without email verification
  - Many services analyzed
  - Identified as vulnerable:

CloudMe

Dropbox

wuala by LACIE

HiDrive

IDrive® Did you back it up?™

syncplicity

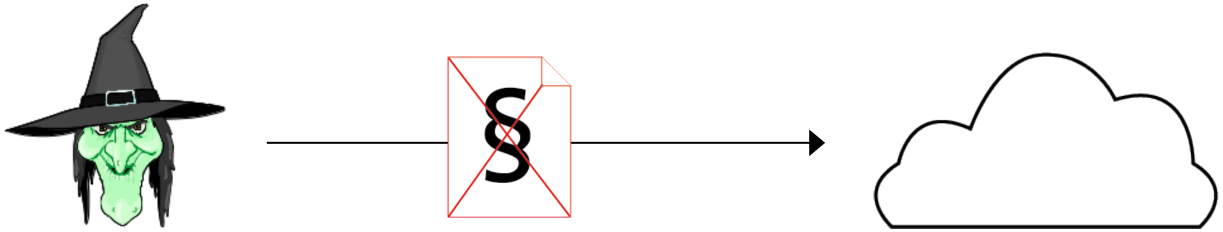
SugarSync

Security Issues: Unverified email addresses

- Several services allow registration without email verification
  - Incrimination attack
    1. Attacker registers using email of victim

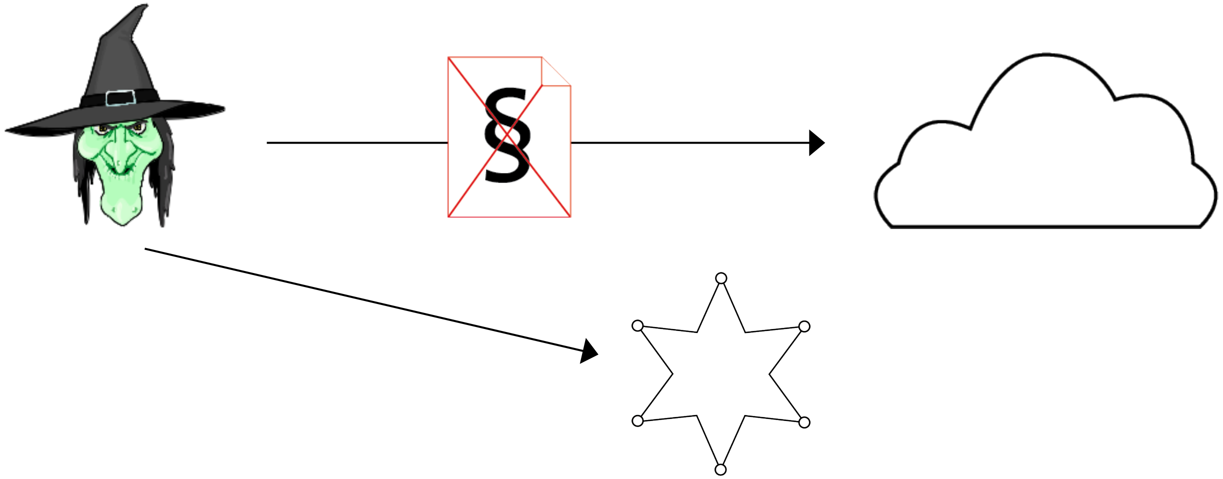
Security Issues: Unverified email addresses

- Several services allow registration without email verification
  - Incrimination attack
    1. Attacker registers using email of victim
    2. Attacker uploads incriminating data



Security Issues: Unverified email addresses

- Several services allow registration without email verification
  - Incrimination attack
    1. Attacker registers using email of victim
    2. Attacker uploads incriminating data
    3. Attacker reports to third party

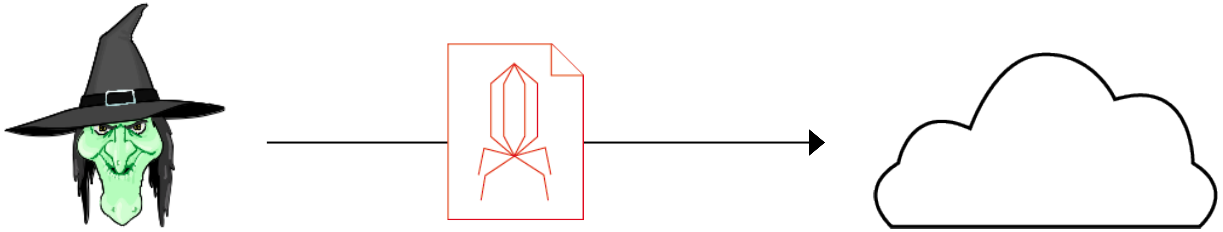


Security Issues: Unverified email addresses

- Several services allow registration without email verification
  - Malware attack
    1. Attacker registers using email of impersonated

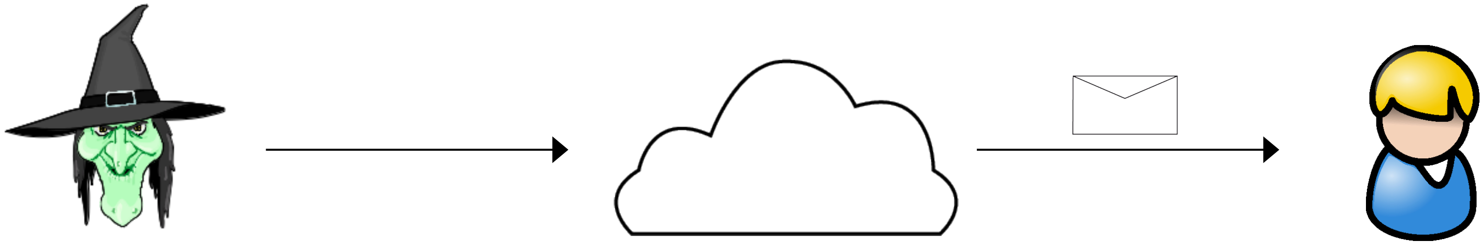
Security Issues: Unverified email addresses

- Several services allow registration without email verification
  - Malware attack
    1. Attacker registers using email of impersonated
    2. Attacker uploads malware



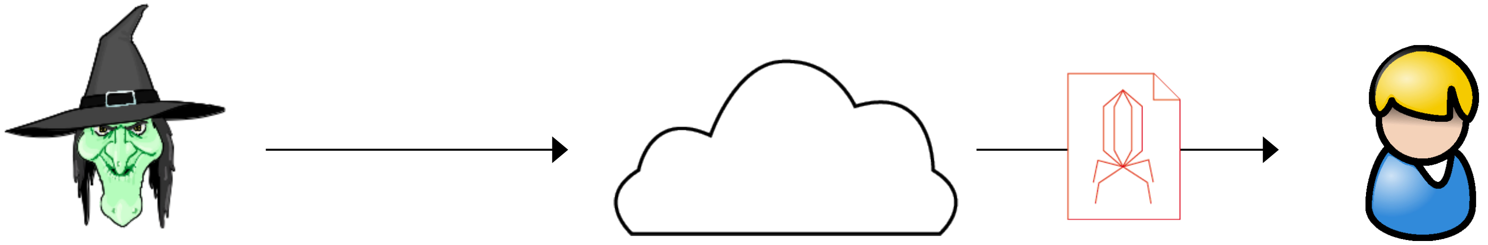
Security Issues: Unverified email addresses

- Several services allow registration without email verification
  - Malware attack
    1. Attacker registers using email of impersonated
    2. Attacker uploads malware
    3. Attacker uses sharing to offer data to victim (friend of impersonated)



Security Issues: Unverified email addresses

- Several services allow registration without email verification
  - Malware attack
    1. Attacker registers using email of impersonated
    2. Attacker uploads malware
    3. Attacker uses sharing to offer data to victim (friend of impersonated)
    4. Victim downloads data

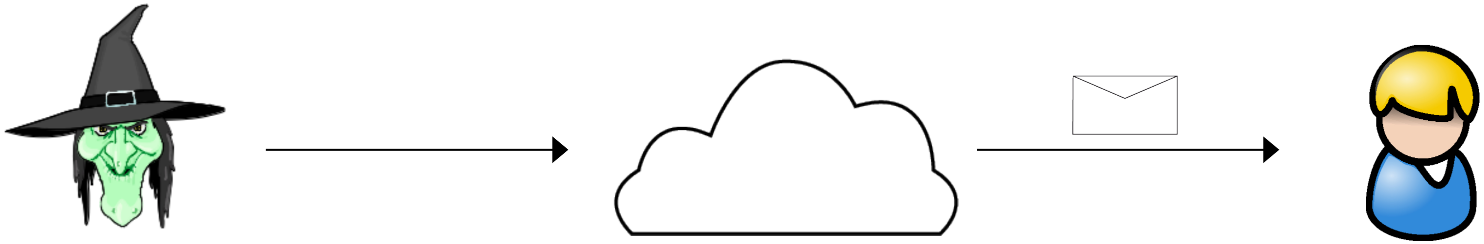


Security Issues: Unverified email addresses

- Several services allow registration without email verification
  - Espionage attack
    1. Attacker registers using email of impersonated

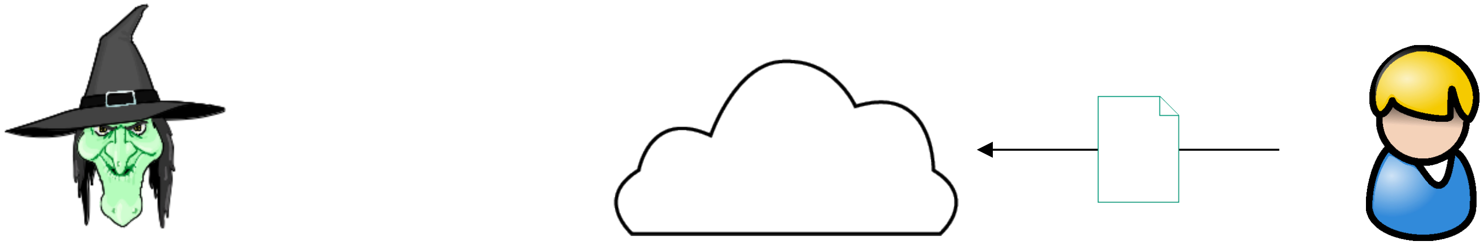
Security Issues: Unverified email addresses

- Several services allow registration without email verification
  - Espionage attack
    1. Attacker registers using email of impersonated
    2. Attacker uses sharing to request data from victim (friend of impersonated)



Security Issues: Unverified email addresses

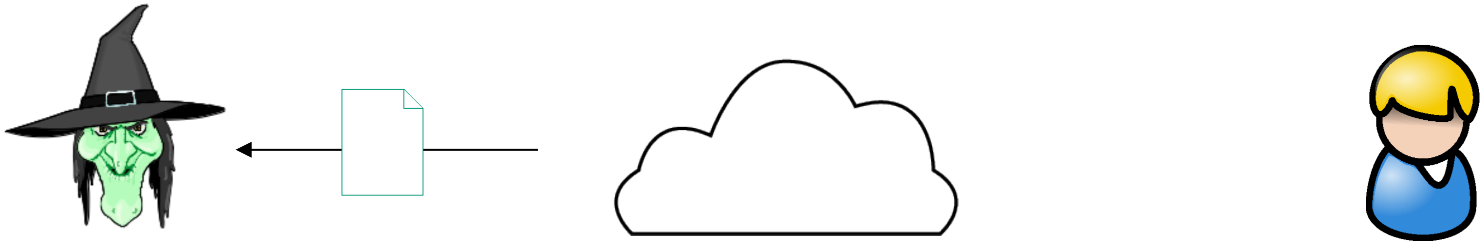
- Several services allow registration without email verification
  - Espionage attack
    1. Attacker registers using email of impersonated
    2. Attacker uses sharing to request data from victim (friend of impersonated)
    3. Victim uploads requested data



© Fraunhofer-Gesellschaft 2012

Security Issues: Unverified email addresses

- Several services allow registration without email verification
  - Espionage attack
    1. Attacker registers using email of impersonated
    2. Attacker uses sharing to request data from victim (friend of impersonated)
    3. Victim uploads requested data
    4. Attacker downloads data



© Fraunhofer-Gesellschaft 2012

Security Issues: Unverified email addresses

- Several services allow registration without email verification
  - How could this happen?
    - Most popular service introduced flaw
    - Other services followed
  - Security at the cost of Usability
    - Streamlined registration process
    - Subsequent introduction of sharing functionality
      - allowed attacks
  - Mitigation strategy
    - Verify email address by sending activation link

Code of Conduct: Handling security issues

- What did we do with our findings?
  - Responsible disclosure
    - Inform service provider
    - Offer to discuss possible solutions
    - Announce date of publication (3-6 months in the future)
  - Findings throughout 2011

  → May 2012: Published technical report

  → June 2012: Published Paper at IEEE TrustCom 2012

  „Vulnerabilities through Usability Pitfalls in Cloud Services: Security Problems due to Unverified Email Addresses"

Cloud Storage Security
Outline

1. Introduction and overview
2. Features
3. Security requirements
4. Security issues
5. **Trust issues**
6. Drawbacks
7. Choice

Trust Issues

- Cloud Storage Services…
  - … are highly attractive attack targets
  - … employ multiple data redundancy and backup schemes
    - Where is my data?
    - Attack surface
  - … operate internationally
    - No specialized SLAs for most customers
    - Legal issues
      - Sensitive data in off-shore data-centers

→ Server-side encryption acceptable?

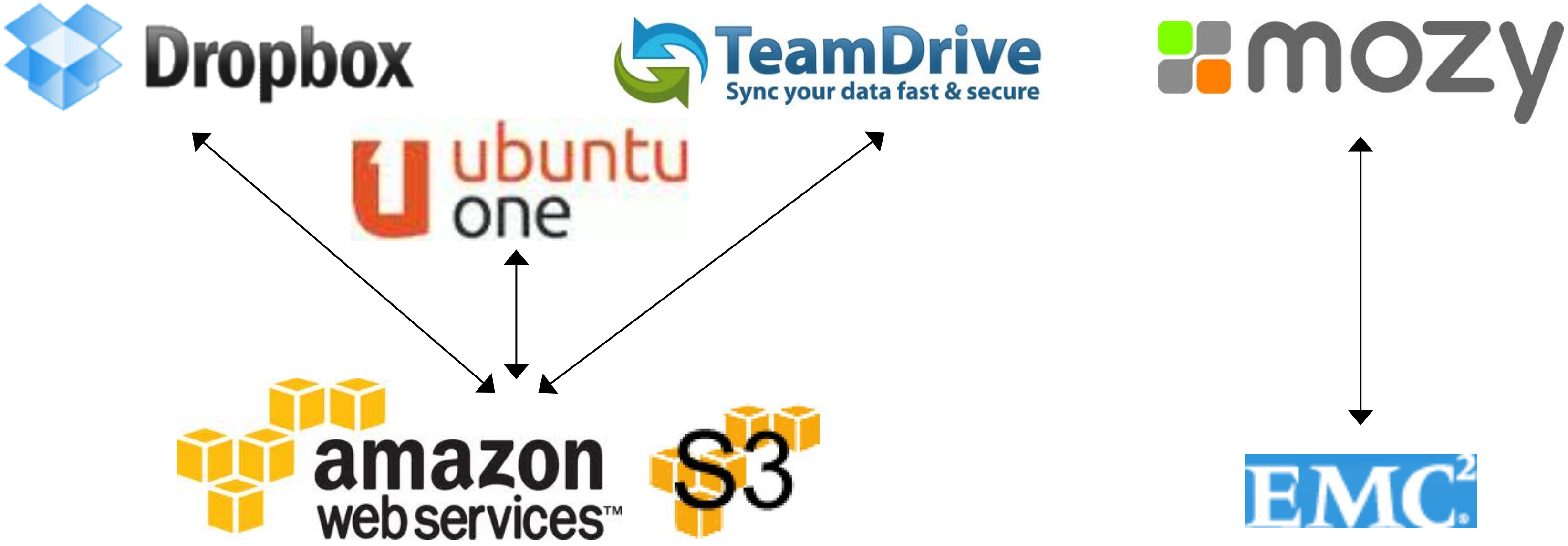
→ Client-side encryption still needs trust !

Trust Issues

- Using the Cloud means
  - Replace on-premise security with trust in provider's ability
  - Replace internal security policy with Service Level Agreement (SLA)
    - But with whom do I effectively deal?

Trust Issues

- Using the Cloud means
  - Replace on-premise security with trust in provider's ability
  - Replace internal security policy with Service Level Agreement (SLA)
    - But with whom do I effectively deal?



Cloud Storage Security
Outline

1. Introduction and overview
2. Features
3. Security requirements
4. Security issues
5. Trust issues
6. **Drawbacks**
7. Choice

Drawbacks of Cloud Storage

- Provider down!
  - Can I cope?
  - Recovery time acceptable?
- Data transmission time
  - Assume 500GB data, download ~1MB/s, upload ~0.25MB/s (DSL 16.000)
    - Upload time estimated: 23.7 days
    - Download time estimated: 5.9 days
- Service provider may go out of business
  - Easy migration possible ?
  - Migration time acceptable?

Cloud Storage Security
Outline

1. Introduction and overview
2. Features
3. Security requirements
4. Security issues
5. Trust issues
6. Drawbacks
7. **Choice**

Choice

- Overview of analysis results

	Registration	Transport	Encryption	Sharing	Deduplication
CloudMe	– –	– –	– –	–	⁒
CrashPlan	+	±	+	⁒	+
Dropbox	–	+	–	±	+
Mozy	±	+	±	⁒	–
TeamDrive	±	±	+	±	⁒
Ubuntu One	+ +	+	– –	+ +	+
Wuala	–	±	±	±	–

Choice

- Choice depends on requirements
  - „Data does not need to be encrypted "
    - i.e. CloudMe, Ubuntu One
  - „Data examination by third parties may be acceptable"
    - i.e. Dropbox
  - „I want client-side encryption and trust my provider"
    - i.e. CrashPlan, Mozy, TeamDrive, (Wuala)
  - „I want everything"
    - No service meets all of our security requirements

Choice

- Cloud Storage Service providers…
  - … are aware of privacy and confidentiality needs
  - … have taken steps to provide high security level
  - … actively try to improve their services
  - … have mostly upgraded their systems to address security issues
- Users need to evaluate…
  - … security level of own data
  - … necessary service functionality

Thank You for your attention ☺

Questions ?