

# Clouds & Security

SBA Research  
Edgar R. Weippl

# Data Storage

## Simple systems

- FTP, WebDAV, NFS

## More complex systems

### A little more complex

- Delta sync
- P2P

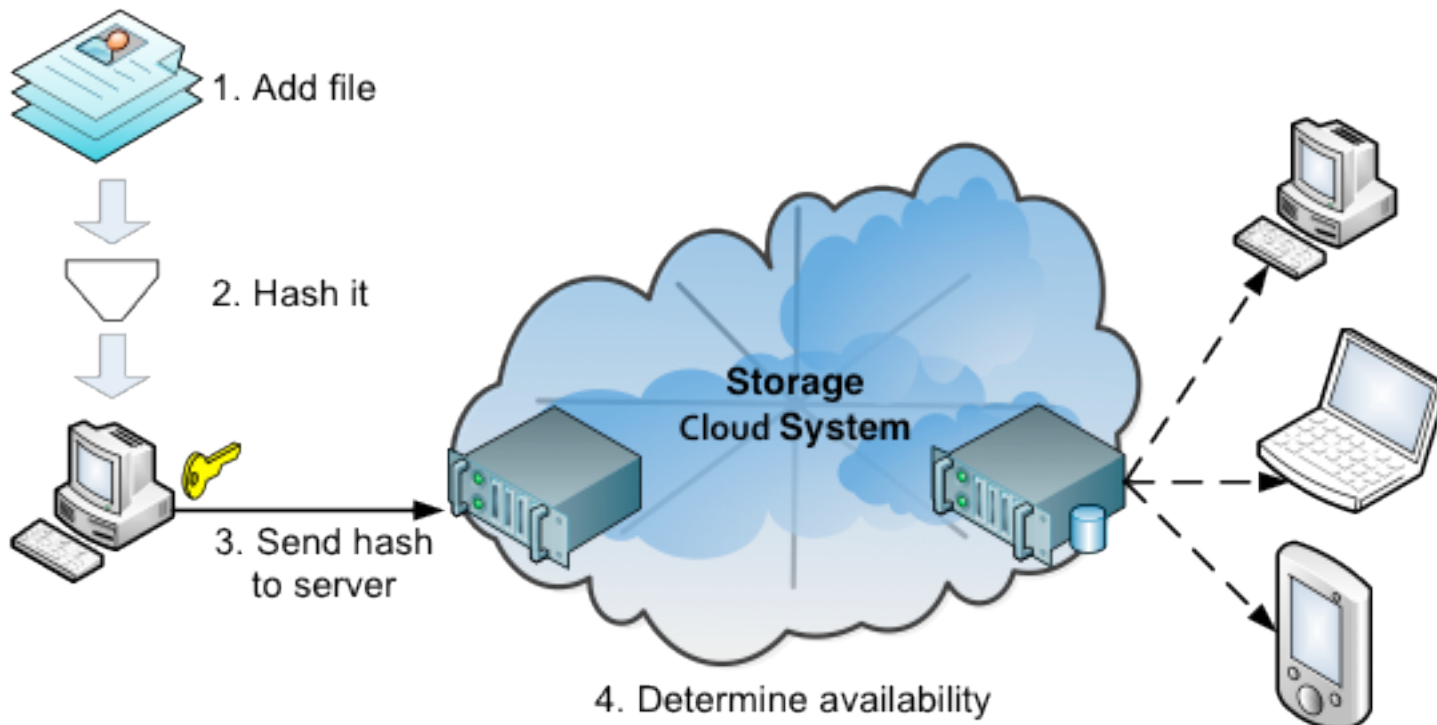
Name	Protocol	Encrypted transmission	Encrypted storage	Shared storage
Wuala	Cryptree	yes	yes	yes
SpiderOak	proprietary	yes	yes	yes
Ubuntu One	u1storage	yes	no	yes
Dropbox	proprietary	yes	no	yes



- uses Amazon Simple Storage System (S3)
- data deduplication, using SHA-256
- files split in 4 MB chunks
- (server-side) AES-256
  
- 25 million users
- Store more than 100 billion files
- 1 million files added every 5 minutes

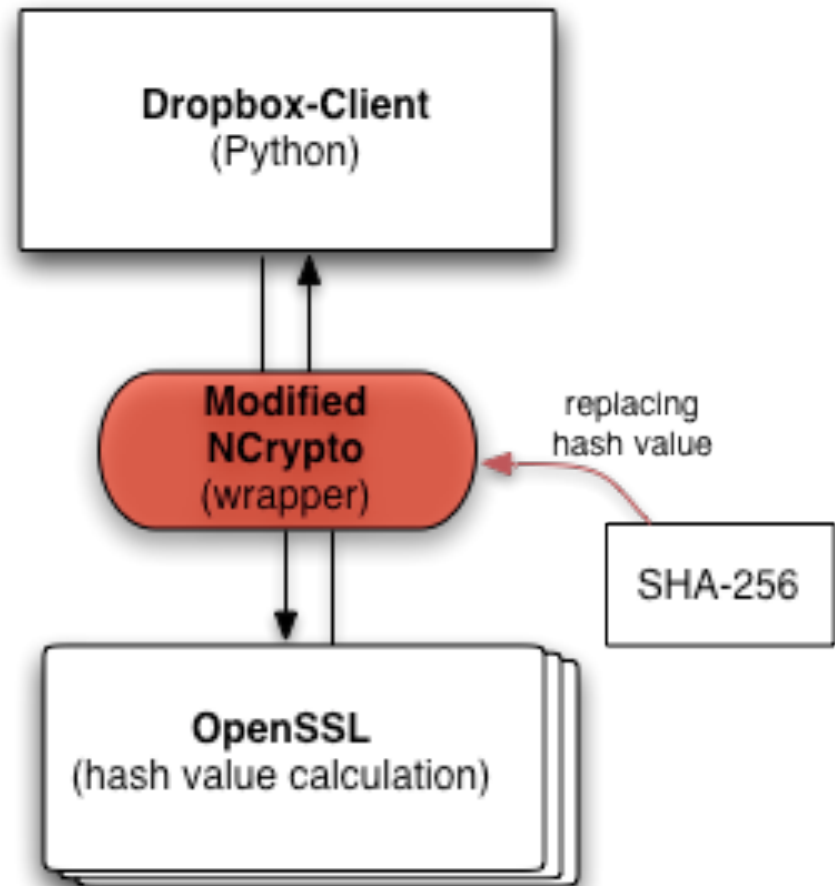
# Data Deduplication

- At the server
  - Same file only stored once
  - Save storage space at server
- At the client
  - Calculate hash or other digest
  - Reduce communication



# Attacks

- Hash manipulation
- Stolen Host ID
- Direct Up-/Download
  - Uploading without linking
  - Simple HTTPS request `https://dl-clientXX.dropbox.com/store`



# Evaluation

Time until (hidden) chunks get **deleted:**

- Random data in multiple files
- Hidden upload: at least 4 weeks
- Regular upload: unlimited undelete possible (> 6 months)

**Popular files on Dropbox:**

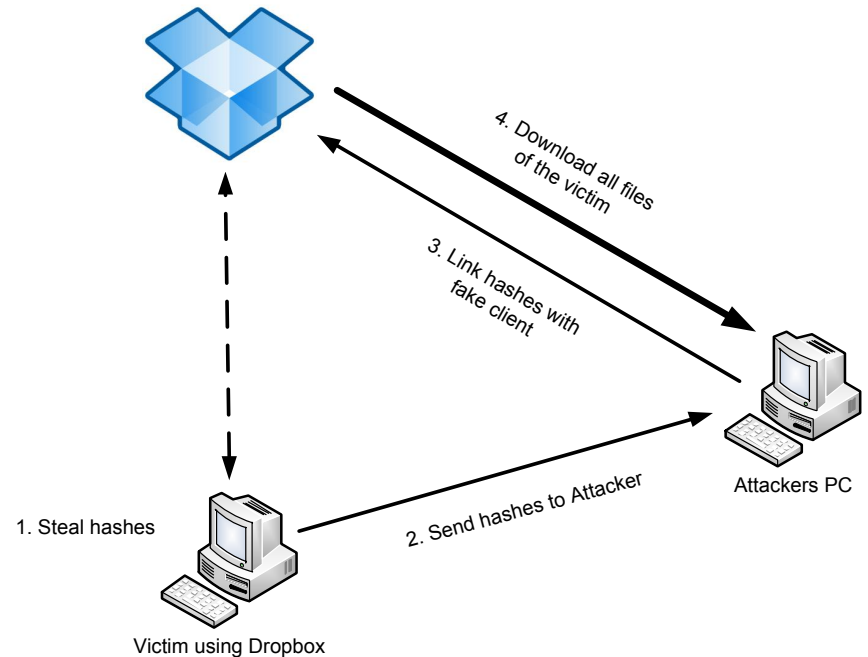
- thepiratebay.org  
Top 100 Torrent files
- Downloaded copyright-free content (.sfv, .nfo, ...)
- 97 % (n = 368) were retrievable
- 20 % of torrents were less than 24 hours old

**Interpretation:**

- At least one of the seeders uses Dropbox

# Solutions

- Aftermath – Dropbox reacted in April
  - HTTPS Up-/Download Attack
  - Host ID is now encrypted
  - No more client-side deduplication
    - Proof of ownership
    - Take down notice



# Contact information

## **Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space,**

Martin Mulazzani, Sebastian Schrittwieser, Manuel Leithner, Markus Huber, and Edgar Weippl

<http://www.usenix.org/events/sec11/tech/>

**Edgar Weippl**

**[www.sba-research.org](http://www.sba-research.org)**

## Our four areas

## Our 13 research projects

---

### Area 1 (GRC): Governance, Risk and Compliance

- P1.1: Risk Management and Analysis
- P1.2: Secure BP Modeling, Simulation and Verification
- P1.3: Computer Security Incident Response Team
- P1.4: Awareness and E-Learning

### Area 2 (DSP): Data Security and Privacy

- P2.1: Privacy Enhancing Technologies
- P2.2: Enterprise Rights Management
- P2.3: Digital Preservation

### Area 3 (SCA): Secure Coding and Code Analysis

- P3.1: Malware Detection and Botnet Economics
- P3.2: Systems and Software Security
- P3.3: Digital Forensics

### Area 4 (HNS): Hardware and Network Security

- P4.1: Hardware Security and Differential Fault Analysis
- P4.2: Pervasive Computing
- P4.3: Network Security of the Future Internet