Chasm: Fault-Tolerant, Information-Theoretic Secure Cloud Back

Alex Grinman, Akshay Ravikumar, Julian Fuchs, Kevin Li

I'm sure there are plenty of existing "secure" back-up solutions…so why?

- **Existing Secure Back-up Solutions:**
  - TBD > Kevin
- **Bad usability:**
  - Passwords (to remember & forget)
  - Keys (to lose when computer crashes, or you write it down and someone steals it)
- **Bad Security**
  - what is the threat model?

Threat model

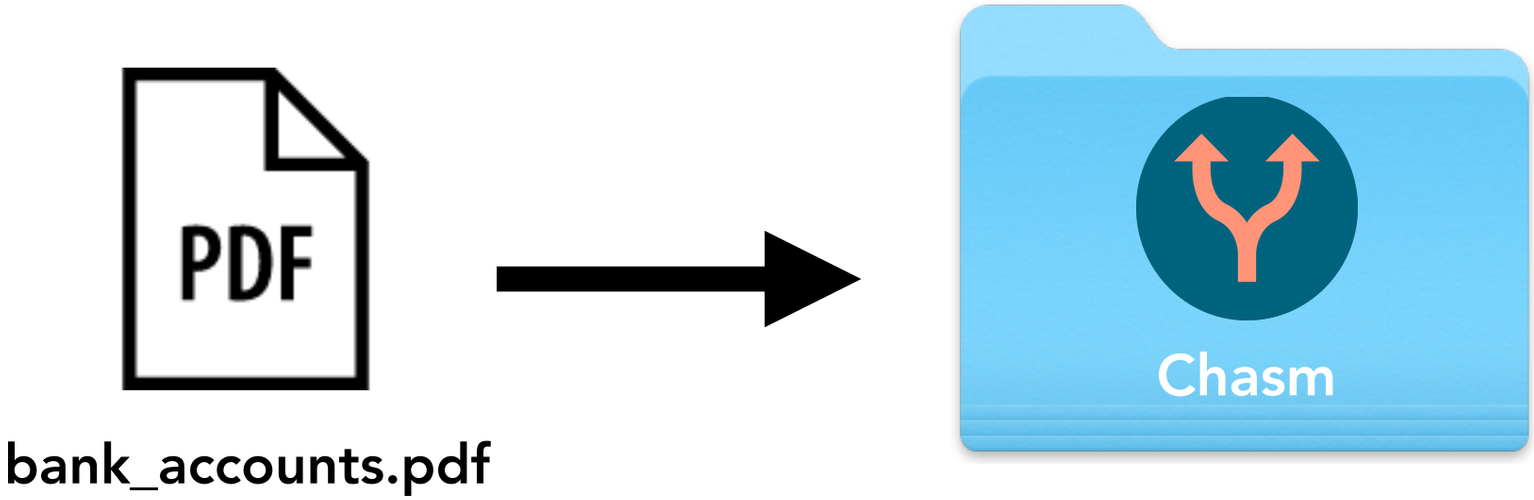
- **Adversaries:**
    1. Cloud Storage Service is curious, wants to gather information to sell
    2. Nation state compels Cloud Service to reveal user data by means of law
    3. Hacker's break into a Cloud Service and steals user
- **Threats:**
    - Cloud Services are computationally powerful!
    - Can Brute force passwords or password-derived encryption keys
    - Denial-of-Service by removing access to encrypted/ plaintext data

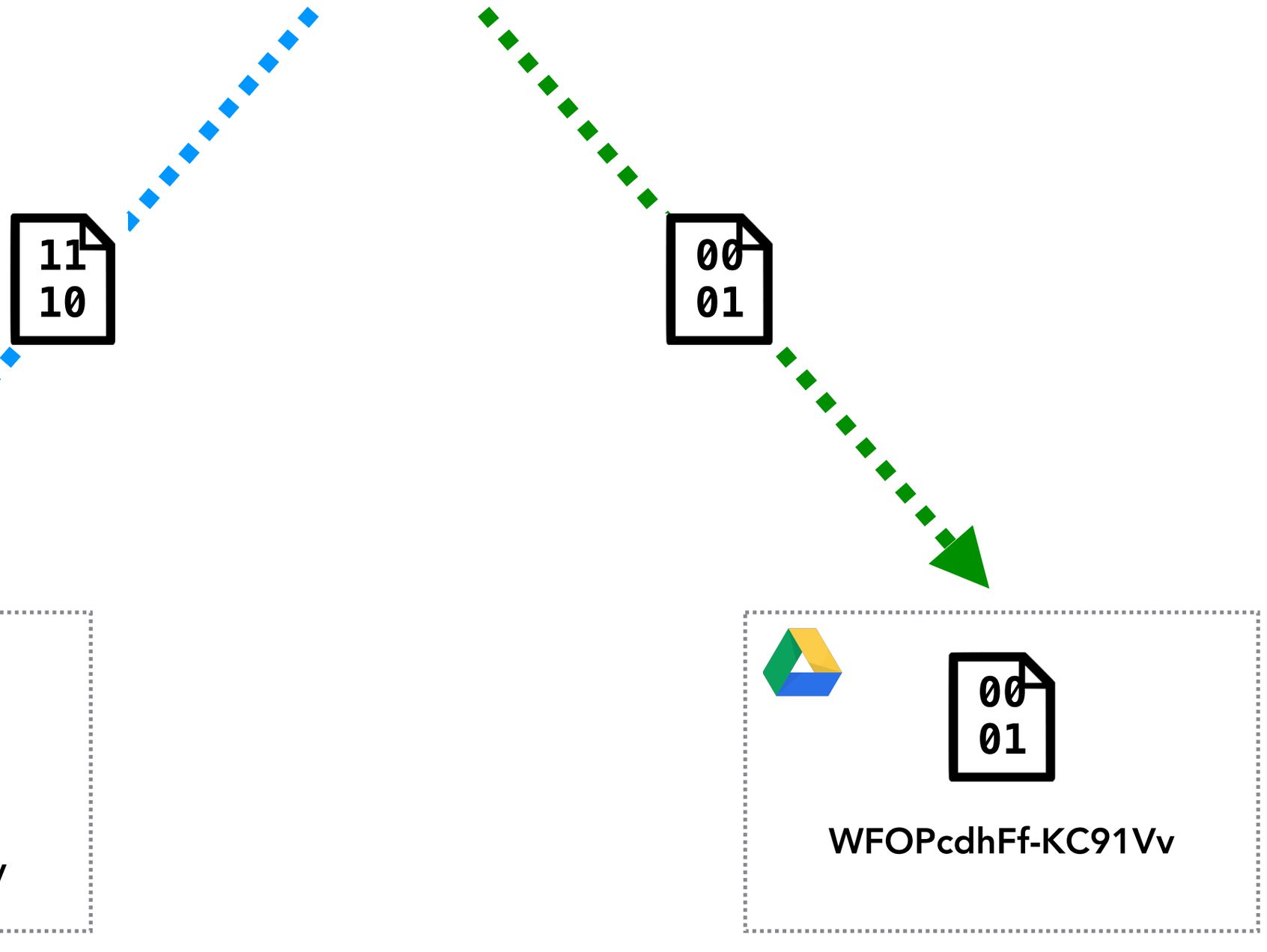
How does Chasm work?

1. **You** specify **> 2** cloud stores like:
    - Dropbox
    - Google Drive
    - iCloud Drive
    - Microsoft One Drive
    - AWS
2. **Chasm** creates a “secure” **chasm folder** in your home directory
3. **You** can now simply drag & drop files into the folder

How does Chasm work?

- Chasm listens for file-system events on the **chasm folder**
- When a new file is added to the **chasm folder**, the file is secret shared using a **K-out-of-N** Shamir's **Secret Sharing Scheme**
- Each share is sent to a different cloud store
- **N** = # of cloud stores
- **K** = recoverability threshold (by default **N**)


PDF
bank_accounts.pdf
Chasm


11
10
00
01
11
10
WFOPcdhFf-KC91Vv
00
01
WFOPcdhFf-KC91Vv

DEMO TIME!

System Guarantees

- **Information-Theoretic Confidentially** of data if less than K-out-of-N cloud services collude

- **Fault-tolerance** lost data is recoverable if at least K-out-of-N cloud services available

- **Integrity** of data if less than K-out-of-N cloud services corrupt shares

Win on Usability

- No passwords to remember
- Easy setup & restore
- Drag & drop to secure
- Most user's already have existing cloud services like Dropbox, Drive, iCloud, etc…

Vulnerabilities
(& how we can fix some of them)

- Cloud stores can determine the number of files and the size of each file
  - Use fixed size blocks!
- A network adversary can potentially combine outbound shares as they are being sent
  - Most cloud stores operate over TLS
- I use the same password for everything?
  - …please turn on 2FA.

Related Systems

- TBD > Kevin

Questions?