SIL765: Network & System Security

Agastya Nanda - 2011MCS2565
Jagmeet Singh Bali - 2011MCS2573

Indian Institute of Technology Delhi

Introduction

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. 2011.

In Proceedings of the 20th USENIX conference on Security (SEC'11). USENIX Association, Berkeley, CA, USA, 5-5.

Introduction

- Large no. of online file storage services

Introduction

- Large no. of online file storage services
- eg., *Dropbox*

Introduction

- Large no. of online file storage services
- eg., *Dropbox*
  - Over 1 billion files as of May 2011

Introduction

- Large no. of online file storage services
- eg., *Dropbox*
  - Over 1 billion files as of May 2011
  - Saves 1 million files every 5 minutes

Introduction

- Large no. of online file storage services
- eg., *Dropbox*
  - Over 1 billion files as of May 2011
  - Saves 1 million files every 5 minutes
- Advanced Features:

Introduction

- Large no. of online file storage services
- eg., *Dropbox*
  - Over 1 billion files as of May 2011
  - Saves 1 million files every 5 minutes
- Advanced Features:
  - Shared Folders

Introduction

- Large no. of online file storage services
- eg., *Dropbox*
  - Over 1 billion files as of May 2011
  - Saves 1 million files every 5 minutes
- Advanced Features:
  - Shared Folders
  - Minimize transfer time

Introduction

- Large no. of online file storage services
- eg., *Dropbox*
  - Over 1 billion files as of May 2011
  - Saves 1 million files every 5 minutes
- Advanced Features:
  - Shared Folders
  - Minimize transfer time
  - Unlimited Space

Introduction

- Large no. of online file storage services
- eg., *Dropbox*
  - Over 1 billion files as of May 2011
  - Saves 1 million files every 5 minutes
- Advanced Features:
  - Shared Folders
  - Minimize transfer time
  - Unlimited Space
- $\Longrightarrow$ Disk Space on Servers

Introduction

- Large no. of online file storage services
- eg., *Dropbox*
  - Over 1 billion files as of May 2011
  - Saves 1 million files every 5 minutes
- Advanced Features:
  - Shared Folders
  - Minimize transfer time
  - Unlimited Space
- $\Longrightarrow$ Disk Space on Servers
- Server-side data deduplication

Dropbox Internals

- No concept of files.

Dropbox Internals

- No concept of files.
- Files split into Chunks of 4MB

Dropbox Internals

- No concept of files.
- Files split into Chunks of 4MB
- Hash value of each Chunk (*SHA-256*)

Dropbox Internals

- No concept of files.
- Files split into Chunks of 4MB
- Hash value of each Chunk (*SHA-256*)
- While uploading:

Dropbox Internals

- No concept of files.
- Files split into Chunks of 4MB
- Hash value of each Chunk (*SHA-256*)
- While uploading:
  - Client breaks file into chunks and hashes.

Dropbox Internals

- No concept of files.
- Files split into Chunks of 4MB
- Hash value of each Chunk (*SHA-256*)
- While uploading:
  - Client breaks file into chunks and hashes.
  - If file of same hash already exists on server, linked to user.

Dropbox Internals

- No concept of files.
- Files split into Chunks of 4MB
- Hash value of each Chunk (*SHA-256*)
- While uploading:
  - Client breaks file into chunks and hashes.
  - If file of same hash already exists on server, linked to user.
  - $\implies$ saves traffic and storage costs.

Dropbox Internals

- No concept of files.
- Files split into Chunks of 4MB
- Hash value of each Chunk (*SHA-256*)
- While uploading:
  - Client breaks file into chunks and hashes.
  - If file of same hash already exists on server, linked to user.
  - $\implies$ saves traffic and storage costs.
- Connections secured by SSL

Dropbox Internals

- No concept of files.
- Files split into Chunks of 4MB
- Hash value of each Chunk (*SHA-256*)
- While uploading:
  - Client breaks file into chunks and hashes.
  - If file of same hash already exists on server, linked to user.
  - $\implies$ saves traffic and storage costs.
- Connections secured by SSL
- Uploaded data stored on Amazon S3 storage service.

Unauthorized File Access

- Hash Value Manipulation

Unauthorized File Access

- Hash Value Manipulation
- Stolen Host ID

Unauthorized File Access

- Hash Value Manipulation
- Stolen Host ID
- Direct Download

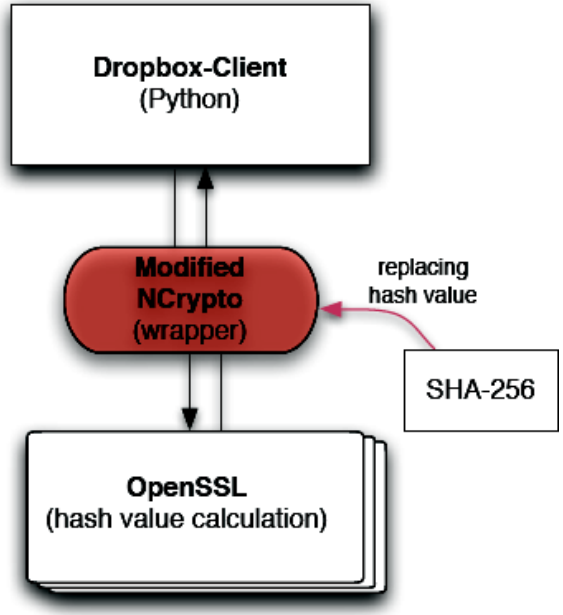
Unauthorized File Access

- Hash Value Manipulation
- Stolen Host ID
- Direct Download

- Owner of file unable to detect attackers accessing the file.

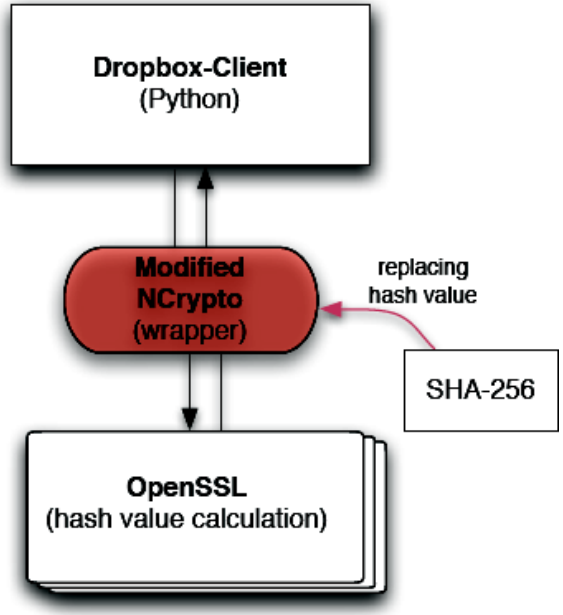
Hash Value Manipulation Attack

- Modify library that Client uses (NCrypto)



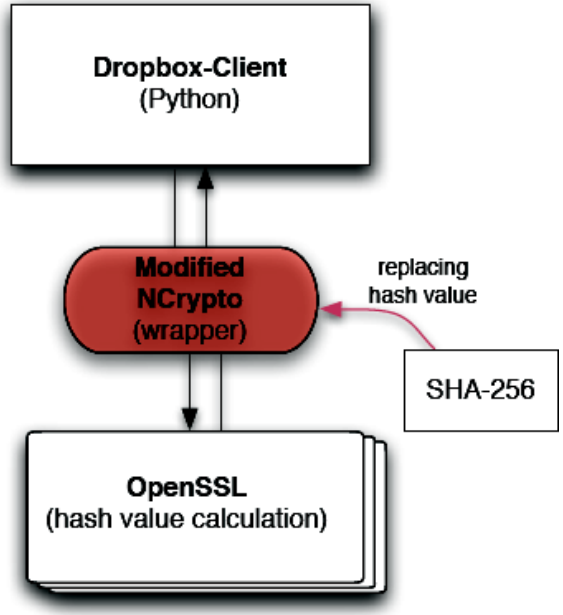
Hash Value Manipulation Attack

- Modify library that Client uses (NCrypto)
- Use client to request upload



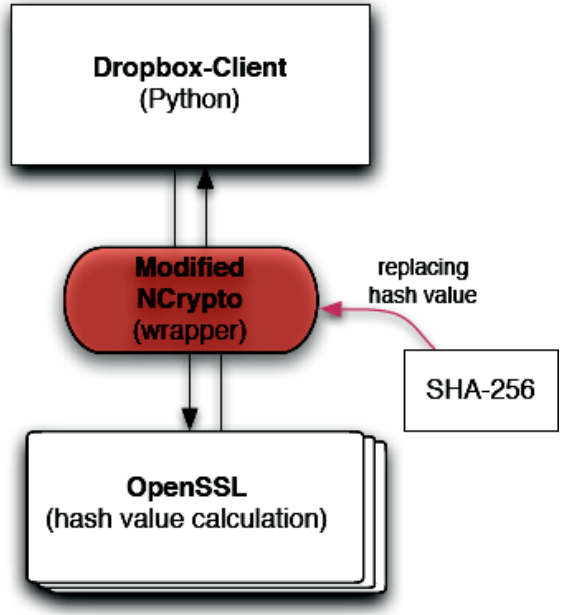
Hash Value Manipulation Attack

- Modify library that Client uses (NCrypto)
- Use client to request upload
- Send *our own* generated SHA-256 hash to server



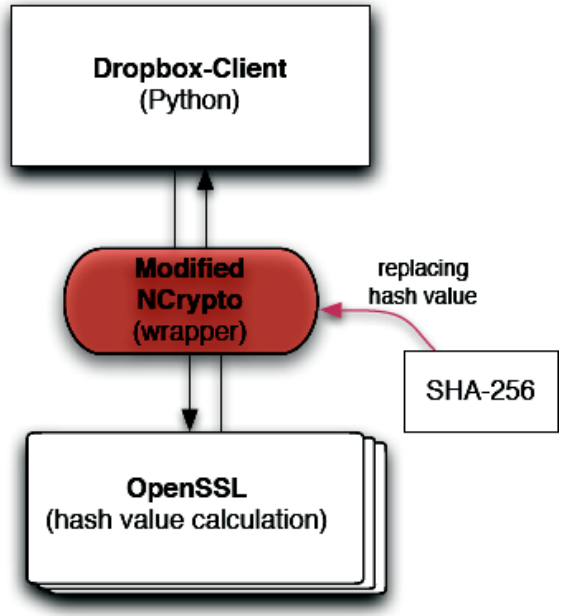
Hash Value Manipulation Attack

- Modify library that Client uses (NCrypto)
- Use client to request upload
- Send *our own* generated SHA-256 hash to server
- If that hash already exists on server, then server does not request file transfer.



Hash Value Manipulation Attack

- Modify library that Client uses (NCrypto)
- Use client to request upload
- Send *our own* generated SHA-256 hash to server
- If that hash already exists on server, then server does not request file transfer.
- Instead the corresponding file/chunk on server is linked to the client



Stolen Host ID Attack

- **Host ID** links specific device running the client to the owner's Dropbox A/C.

Stolen Host ID Attack

- **Host ID** links specific device running the client to the owner's Dropbox A/C.
- 128 bit key (Algorithm not public)

Stolen Host ID Attack

- **Host ID** links specific device running the client to the owner's Dropbox A/C.
- 128 bit key (Algorithm not public)
- Host ID is used for client user authentication

Stolen Host ID Attack

- **Host ID** links specific device running the client to the owner's Dropbox A/C.
- 128 bit key (Algorithm not public)
- Host ID is used for client user authentication
- If obtained using malware, social engineering, etc., can gives access to all user files.

Direct Download Attack

- transmission protocol between client and server is built on HTTPS

Direct Download Attack

- transmission protocol between client and server is built on HTTPS
- Client can request file chunks from https://dl-clientXX.dropbox.com/retrieve

Direct Download Attack

- transmission protocol between client and server is built on HTTPS
- Client can request file chunks from https://dl-clientXX.dropbox.com/retrieve
- Send Hash value and *ANY* valid Host ID as POST data

Online Slack Space

- Uploading file similar to downloading with HTTPS

Online Slack Space

- Uploading file similar to downloading with HTTPS
- Client calls https://dl-clientXX.dropbox.com/store

Online Slack Space

- Uploading file similar to downloading with HTTPS
- Client calls https://dl-clientXX.dropbox.com/store
- Send hash value and host ID as HTTPS POST along with actual data.

Online Slack Space

- Uploading file similar to downloading with HTTPS
- Client calls https://dl-clientXX.dropbox.com/store
- Send hash value and host ID as HTTPS POST along with actual data.
- After upload, the client software links the uploaded files to the host ID with another HTTPS request

Online Slack Space

- Uploading file similar to downloading with HTTPS
- Client calls https://dl-clientXX.dropbox.com/store
- Send hash value and host ID as HTTPS POST along with actual data.
- After upload, the client software links the uploaded files to the host ID with another HTTPS request
- Modified client can upload unlimited data if linking step is omitted.

Attack Vector

- If host ID is known to attacker

Attack Vector

- If host ID is known to attacker
- Modified client can upload malicious data and *link* to victim's host ID.

Attack Vector

- If host ID is known to attacker
- Modified client can upload malicious data and *link* to victim's host ID.
- Can be used in conjunction with OS file preview bug.

Attack Vector

- If host ID is known to attacker
- Modified client can upload malicious data and *link* to victim's host ID.
- Can be used in conjunction with OS file preview bug.
- When victim "previews" malicious file ...

Results

- Long term undelete

Results

- Long term undelete
  - uploaded 55 files with a regular Dropbox account and deleted them right afterwards (Oct 7, 2010)

Results

- Long term undelete
  - uploaded 55 files with a regular Dropbox account and deleted them right afterwards (Oct 7, 2010)
  - Checked for any "Garbage Collection"

Results

- Long term undelete
  - uploaded 55 files with a regular Dropbox account and deleted them right afterwards (Oct 7, 2010)
  - Checked for any "Garbage Collection"
  - Until Dropbox fixed the HTTPS download attack at the end of April 2011, 100% had been constantly available.

Results

- Long term undelete
  - uploaded 55 files with a regular Dropbox account and deleted them right afterwards (Oct 7, 2010)
  - Checked for any "Garbage Collection"
  - Until Dropbox fixed the HTTPS download attack at the end of April 2011, 100% had been constantly available.
- Online Slack

Results

- Long term undelete
  - uploaded 55 files with a regular Dropbox account and deleted them right afterwards (Oct 7, 2010)
  - Checked for any "Garbage Collection"
  - Until Dropbox fixed the HTTPS download attack at the end of April 2011, 100% had been constantly available.
- Online Slack
  - uploaded 30 files of various sizes without linking them to any account

Results

- Long term undelete
  - uploaded 55 files with a regular Dropbox account and deleted them right afterwards (Oct 7, 2010)
  - Checked for any "Garbage Collection"
  - Until Dropbox fixed the HTTPS download attack at the end of April 2011, 100% had been constantly available.
- Online Slack
  - uploaded 30 files of various sizes without linking them to any account
  - 4 weeks later all files were still retrievable

Results

- Long term undelete
  - uploaded 55 files with a regular Dropbox account and deleted them right afterwards (Oct 7, 2010)
  - Checked for any "Garbage Collection"
  - Until Dropbox fixed the HTTPS download attack at the end of April 2011, 100% had been constantly available.
- Online Slack
  - uploaded 30 files of various sizes without linking them to any account
  - 4 weeks later all files were still retrievable
  - When Dropbox fixed the HTTPS download attack in late April 2011, 50% of the files were still available.

Countermeasures

- secure data possession protocol should be used to prevent the clients to get access to files only by knowing the hash value of a file

Countermeasures

- secure data possession protocol should be used to prevent the clients to get access to files only by knowing the hash value of a file
- No chunks without Linking

Countermeasures

- secure data possession protocol should be used to prevent the clients to get access to files only by knowing the hash value of a file
- No chunks without Linking
- Check for host ID activity – Prevent access if host is not online

Countermeasures

- secure data possession protocol should be used to prevent the clients to get access to files only by knowing the hash value of a file
- No chunks without Linking
- Check for host ID activity – Prevent access if host is not online
- dynamic host ID would reduce the window of opportunity that an attacker could use to clone a victim's Dropbox by stealing the host ID.

Countermeasures

- secure data possession protocol should be used to prevent the clients to get access to files only by knowing the hash value of a file
- No chunks without Linking
- Check for host ID activity – Prevent access if host is not online
- dynamic host ID would reduce the window of opportunity that an attacker could use to clone a victim's Dropbox by stealing the host ID.
- Dropbox should keep track of which files are in which Dropboxes (enforcement of data ownership)

Thank You