



On the privacy of File Sharing Services

OWASP

Nick Nikiforakis

Katholieke Universiteit Leuven, Belgium

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation

<http://www.owasp.org>

Who am I?

- Nick Nikiforakis
- PhD student in KUL
- Security research
 - ▶ Low-level
 - ▶ Web application
- <http://www.securitee.org>

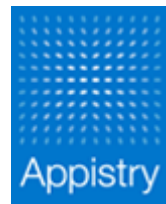
One sentence

- File Sharing websites and privacy do not mix well. If you must use them, select them wisely...

Outline

- The Cloud
- File Sharing Services
 - ▶ Workings
 - ▶ Token Generation
 - ▶ Privacy
- Enumeration
- Results
- Security issues
- Conclusion

The Cloud...



What is the cloud?

- Shared resources on demand
- Pay-as-you-go style
- No need for small/medium company to buy and create their own infrastructures
 - Great for startups
 - Not so great for private data



When the cloud turns gray

■ Data losses

- ▶ 2007: Amazon EC2
 - Customer Application Data
- ▶ 2009: Microsoft: T-Mobile Sidekick data
 - SMS, Calendars, pictures etc.
 - “likely lost all user data that was being stored on Microsoft’s servers due to a server failure”

■ Privacy

- ▶ Chrome OS
- ▶ Google Printing Service

File Sharing Services

- Cloud storage for the masses
- One-click hosting
- Mostly anonymous access
 - At least for non-paying users
- Used for sharing both public & private files

FSS Workings

- User chooses a FSS
- Uploads a file through their web interface
 - HTML + JS + FLASH
- The file gets stored in one of the servers of the FSS
- FSS creates a token, assigns it to the file and returns the token to the user in a URL form

Sharing of files through FSS

- Once a file is uploaded it can be shared according to its nature:
 - Private – Link through email, IM, etc. (1-1)
 - Public – Link on forums, blogs, IRC (1-N)

Privacy of FSS

- Protecting files from non-owners
- Security through obscurity
 - Their services are not searchable
 - A user can access a file only if he knows the file's unique and secret identifier



Privacy of FSS

- Protecting files from non-owners
- Security through obscurity
 - Their services are not searchable
 - A user can access a file only if he knows the file's unique and secret identifier



Actual uploads

patterns?!?

<u>Service ID</u>	<u>First Upload</u>	<u>Second Upload</u>
FSS 1	376567678/owasp.zip.html	376567757/owasp.zip.html
FSS 2	/b121h9f/n/owasp_zip	/b121ha7/n/owasp_zip
FSS 3	/1909943800/owasp.zip	/1909943802/owasp.zip
FSS 4	16141045/owasp.zip	16141055/owasp.zip
FSS 5	/2016359	/2016360
FSS 6	/?mозmocgxry5	/?j1jrj0qyden
FSS 7	/file/prsyryj	/file/v1o1sq
FSS 8	/owasp	/owasp_1

Predictability

- Many services generate predictable tokens (URLs)
- Starting from a valid token, an attacker can enumerate the whole database
 - ▶ Access to tens of millions of files
- This doesn't stop on FSS

Specifics

■ FSS2

- ▶ 1909943800, 1909943799, 1909943798...are all valid tokens

■ FSS3

- ▶ b121h9f, b121h9e, b121h9d... are all valid tokens
- ▶ $18^7 > 600,000,000$ files

■ Lets enumerate them!

Enumeration

- One enumerator for each service
 - ▶ Several instances from several IP addresses
 - ▶ Waiting ~10 sec. between requests
 - Defeating blacklisting from possible IDS
 - No Overload
 - 8640 records/per day, per service
 - ▶ Starting from a valid token and subtracting one

- What did we get?

Sneak Peek FSS2

- b00dd1d | 086-091_D04_S14.oneddl.wyxchari._-089_.rar | 374.91 KB
- b00dd1c | ASD.El.Fersaan.Ep38.By.Starz.rar | 106.23 MB
- b00dd1b | DJ_Tiesto-Lethal_Industry-Retail-CDM-2002-MTC_mov-world.net.rar | 54.49 MB
- b00dd1a | D_WAPINZ_-_Hidupku_Seorang_3_.mpg | 25.49 MB
- b00dd19 | 05_-_Fly_With_Me.mp3 | 3.55 MB
- b00dd18 | KunoFch001.rar | 58.49 MB
- b00dd17 | Calle_13_Ft_Mercedes_Sosa_Para_Un_Nino_De_La_Calle_Www.FlowHoT.Net_.mp3 | 4.89 MB
- b00dd16 | [Document.zip](#) | 499.61 KB
- b00dd15 | [DSC_8973.jpg](#) | 6.27 MB

Sneak Peek FSS3

- 1909260240 | [LISTINO LORDO 2010 AGGIORNATO 200110.xls](#) (0.7 MB)
- 1909260239 | Almoraima (BulerÃas).mp3.zip (8.7 MB)
- 1909260238 | Desi_Table.3gp (5.7 MB)
- 1909260237 | Bizim_Same_v1.05_By_USLUBank.rar (4.1 MB)
- 1909260236 | O_Kay_.part4.rar (99.2 MB)
- 1909260235 | [P1010562.JPG](#) (1.5 MB)
- 1909260234 | RecoverMyFiles3.9.8.5966.exe (7.6 MB)
- 1909260233 | [LISTINO LORDO 2010 AGGIORNATO 200110.xls](#) (0.7 MB)
- 1909260232 | [Suigintou_Rozen Maiden.jpg](#) (4.0 MB)

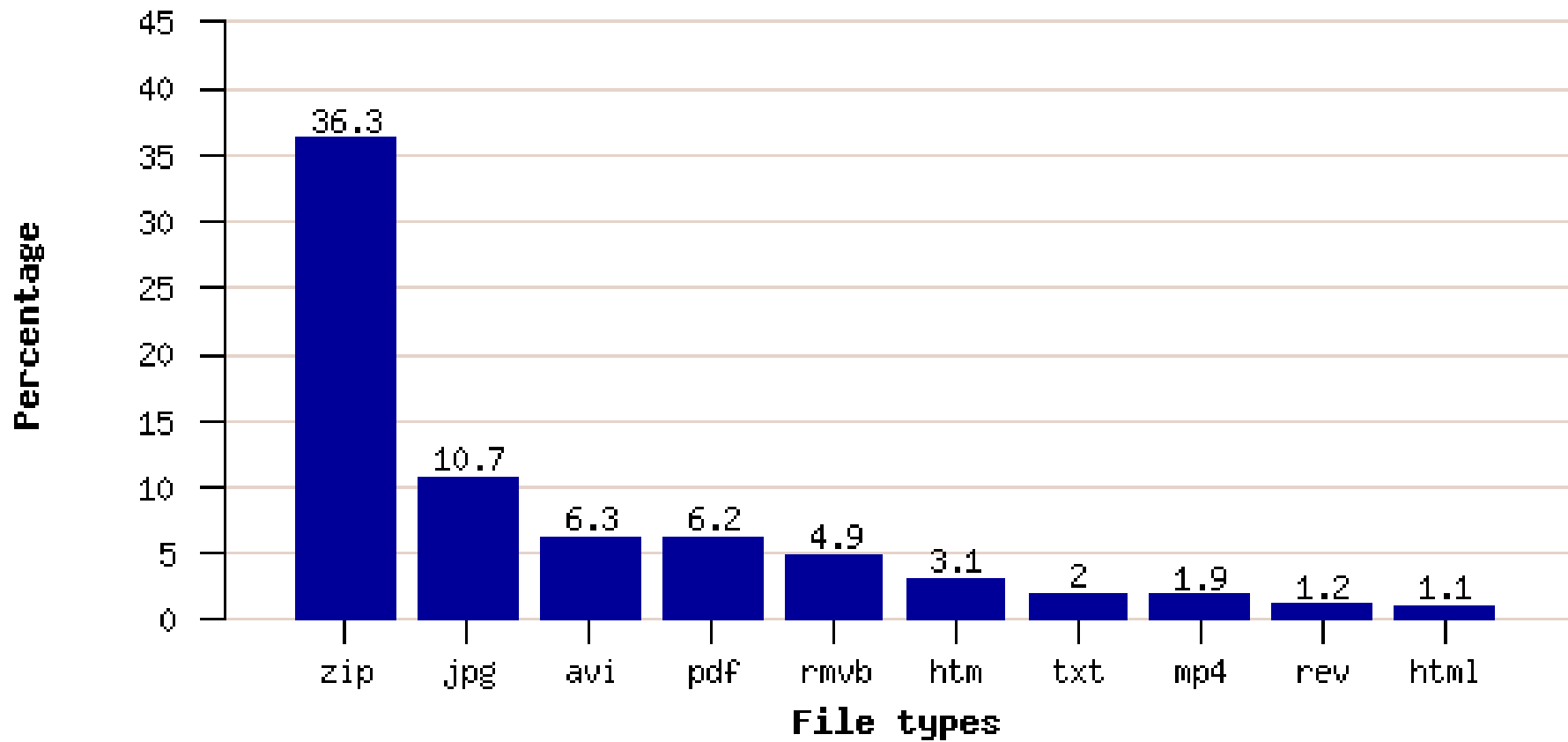
How to find interesting data

- Data is simply too much for manual inspection
- Automatic privacy classification engine
- Google search engine
 - ▶ Search for files on search engines and look at the results
 - ▶ Actually Yahoo! because Google blocked us 😊
 - ▶ 5,000 requests per day

Results

- 1 in 5 files returns no search results
- 30,000 private files... (so far)
 - ▶ Pictures
 - ▶ Documents
 - ▶ Spreadsheets
 - ▶ PHP pages
 - ▶ .sql files
 - ▶ ...

Results



Top10 Private file types

Memorable moments

- Bank statements
- Company Budgets and salaries
- Phones numbers, names, emails, dates of birth
- Death certificate
- Service manual for photo-printer
- 14 documents with doctor-transcribed notes

Attacks made possible

- Identity theft
 - ▶ Private pictures, documents
 - ▶ Personal data
- Scamming
- Server attacks
- Corporate espionage
- Blackmailing



The problem is...

- This is not easily fixable
- Even if the tokens from now on are secure
 - ▶ File Hosting Providers cannot change the tokens for the files that exist so far
- Dilemma
 - ▶ Delete several millions of files
 - And make your customers angry
 - ▶ Keep them...



Protect yourself

- If you must use a FSS:
 - ▶ Choose one which generates truly random tokens
 - ▶ Password-protect your file
 - ▶ Delete it once you have successfully shared it

- Use company policies



Conclusion

- Most file sharing services are insecure
- Minimal effort => Maximum results
- Not easily solvable for existing FSS

Thank you

■ Q&C?



nick.nikiforakis@cs.kuleuven.be

<http://www.securitee.org>