Augmenting Password Recovery with Online Profiling

By

Khawla Al-Wehaibi, Tim Storer and Brad Glisson

Presented At

The Digital Forensic Research Conference

DFRWS 2011 USA New Orleans, LA (Aug 1st - 3rd)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

Augmenting Password Recovery with Online Profiling

Khawla Al-Wehaibi[1] Tim Storer[2] Brad Glisson[3]

[1]Department of Computer & Information Science, Prince Sultan University
[2]School of Computing Science, University of Glasgow
[3]School of Humanities, University of Glasgow

DFRWS 2011 **August 1st 2011**

Outline

- Motivation.
- Research Aim.
- Relevant Studies.
- Method.
- Findings.
- Consideraions.
- Conclusion.

Motivation

- Users' behaviour towards passwords creation:
  - InfoSecurity Europe surveyed 152 participants (2003):
    - 16% use their own names in their passwords.
    - 11% use their football team names.
    - 8% use their date of birth.

Motivation

- Users' behaviour towards passwords creation:
  - Microsoft (2004):
    - One in five (around 20%) individuals use their mother's maiden name in their passwords.
    - One in eight (around 12%) use their football teams.

Motivation

- The problem of encryption and passwords:
  - Rogers and Seigfried (2004):
    - In a pilot study of 60 participants involved in the field of computer forensics, encryption was reported as the 3rd most frequently mentioned issue.
  - User-friendly encryption tools.

Research Aim

- Test whether online information can speed up password recovery compared with a dictionary attack by an industry standard tool.

Relevant Studies

- Fragkos and Tryfonas (2007):
  - Proposed a cognitive model for finding passwords and introduced the concept of Level of Difficulty ‘LoD’.

Relevant Studies

- Spafford (1992):
  - Enhance passwords choices.
  - 13,787 UNIX passwords were collected from the computers in the Department of Computer Sciences & the Computing Center at Purdue University.
  - Experiments lasted for approximately 10 months.
  - 20% passwords were recovered.
  - 3.9% passwords consisted of UNIX accounts' names, users' names or telephone numbers.

Relevant Studies

- Klein (1990):
  - Demonstrate passwords weaknesses.
  - Exposed 13,797 passwords collected from colleagues to dictionary attacks.
  - 24.2% passwords were recovered.
  - 2.7% passwords recovered by using accounts' names and users' names including initials.
  - 7% passwords recovered by using common names, females' names, males' names, places' names, sports terms or teams' names.

Method

- Ethical approval was acquired.
- Participants' password-protected Word documents were collected.
- The web crawler was developed.
- Participants' online information was gathered.
- Dictionary attacks were performed.

Method

- Participants recruitment:
  - An email was sent to faculty members in the School of Computing Science and Humanities Advanced Technology and Information Institute ‘HATII’ at the University of Glasgow.
  - Willing candidates were contacted in person.
  - Participants were asked to password-protect a Microsoft Office 97-2003 Word document with a password they use or have used.
  - No restrictions were imposed on the passwords.

Method

- Participants recruitment:
  - Participants were assured that none of the recovered passwords will be recorded.
  - **23** participants agreed to participate. Six members did not have useful online information, therefore only **17** candidates were eligible for the study (13 members were from the School of Computing Science and 4 members were from HATII). One participant provided two Word documents protected with different passwords ➔**18** Word documents.

Method

- The web crawler:
  - Open source web crawlers ‘ActiveState Code Recipes’.
  - Extracting URLs and saving them in lists.
  - Retrieve web pages’ source code.
  - Filtering the text.
  - Words’ significance.
  - Writing the words.

- The crawler was run on participants’ web pages available in the University of Glasgow website➔ 17 profiles.

Method

- Testing the profiles in PRTK:
  - ‘Microsoft Office Encryption Module’.
  - Password dictionary attacks.
  - PRTK’s rules.
- Three dictionary attacks:
  - PRTK’s dictionaries.
  - Profiles dictionaries.
  - Both.

Method

- The three attacks were performed on the 18 Word documents ➔ 54 attacks.
- Three Word documents were added to two computers and a time-out of 24 hours was set for each attack ➔ 9 working days.

Findings

- Four passwords were recovered:

- Two passwords were recovered by using the profile dictionaries.
- One password was recovered by using the profile dictionary and PRTK's dictionaries.
- One password was recovered twice using two distinct attacks. One attack used PRTK's dictionaries. The other attack used the combined profile dictionary & PRTK's dictionaries.

Findings

File No.	Dictionary used	Time
1	Profile dictionary	10 hr, 24 min & 17 sec
2	Profile dictionary	5 hr, 16 min & 23 sec
3	Profile dictionary and PRTK's dictionaries	4 hr, 53 min & 14 sec
4(a)	Profile dictionary and PRTK's dictionaries	6 hr, 37 min & 53 sec
4(b)	PRTK's dictionaries	6 hr, 53 min & 43 sec

Findings

- The recovery rate (4/18) ≈ 22.2%.
- Klein (1990) recovered 24.2% passwords.
- Spafford (1992) recovered 20% of the passwords.

Considerations

- The depth of the web crawler.
- Participants' websites (quantity & quality of the online information).
- The sample size.
- Passwords' types.

Conclusion

- A web crawler was developed to capture profiles which were then processed by PRTK and dictionary attacks were performed.
- 4 passwords of 18 password-protected Word documents were recovered faster using this technique.

Thank You

Khawla Al-Wehaibi
kwehaibi@yahoo.com