Forensically-Sound Analysis of Security Risks of using Local Password Managers

Joshua Gray University of Derby

Virginia N. L. Franqueira University of Derby

Yijun Yu The Open University (presenter)

iRENIC 2016

@10:30-11:00 September 12, 2016, Friendship Hotel, Beijing, China

UNIVERSITY of DERBY

The Open University

Background

- Passwords remain the most common form of authentication

- A large-scale study (2007)[1] suggests that:
  - A user has, on average, 25 online accounts requiring passwords, and
  - A user types 8 passwords/day

[1] D. Florencio and C. Herley, "A Large-Scale Study of Web Password Habits," in In Proceedings of the 16th International Conference on World Wide Web, WWW'16. ACM Press, 2007, pp. 657–666.

Challenging to remember passwords

- Human capacity to remember passwords is affected by many factors:
  - Password complexity → stronger passwords are harder to remember due to high entropy;
  - Password matching → which password belongs to which account;
  - Frequency of use → rarely used passwords are harder to remember;
  - Frequency of change → periodic changes and history checks exacerbate the problem!

How users cope with the problem?

- Users use different strategies:
  - Reuse passwords
  - Write passwords down
  - Recycle old passwords with small changes
  - Use highly guessable passwords

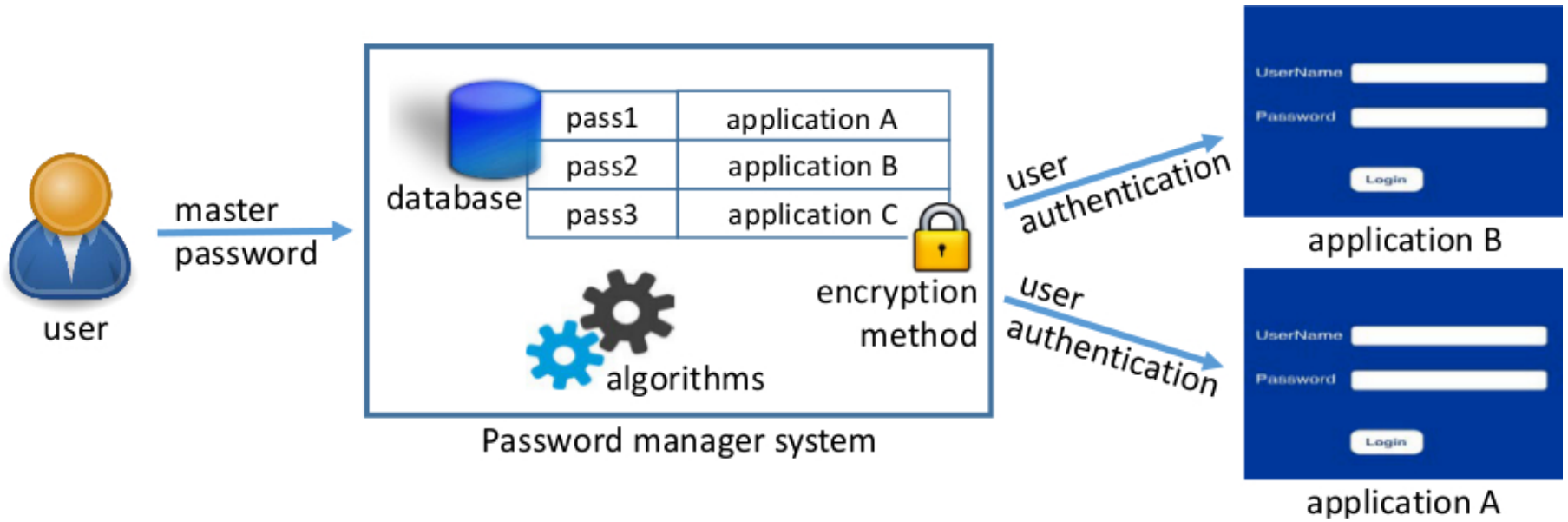
→ These approaches favour usability over security

Solution: Password Managers

- Password Managers have been recommended (e.g., by CERT [7]) as one of the best ways to accommodate the trade-off between usability and security
  - It is becoming best practice for individuals and SMEs

[7] A. Huth, M. Orlando, and L. Pesante, "Password Security, Protection, and Management," United States Computer Emergency Readiness Team, 2012, https://www.us-cert.gov/security-publications/password-security-protection-and-management.

How Password Managers work?



Contexts of use

Scope of this study

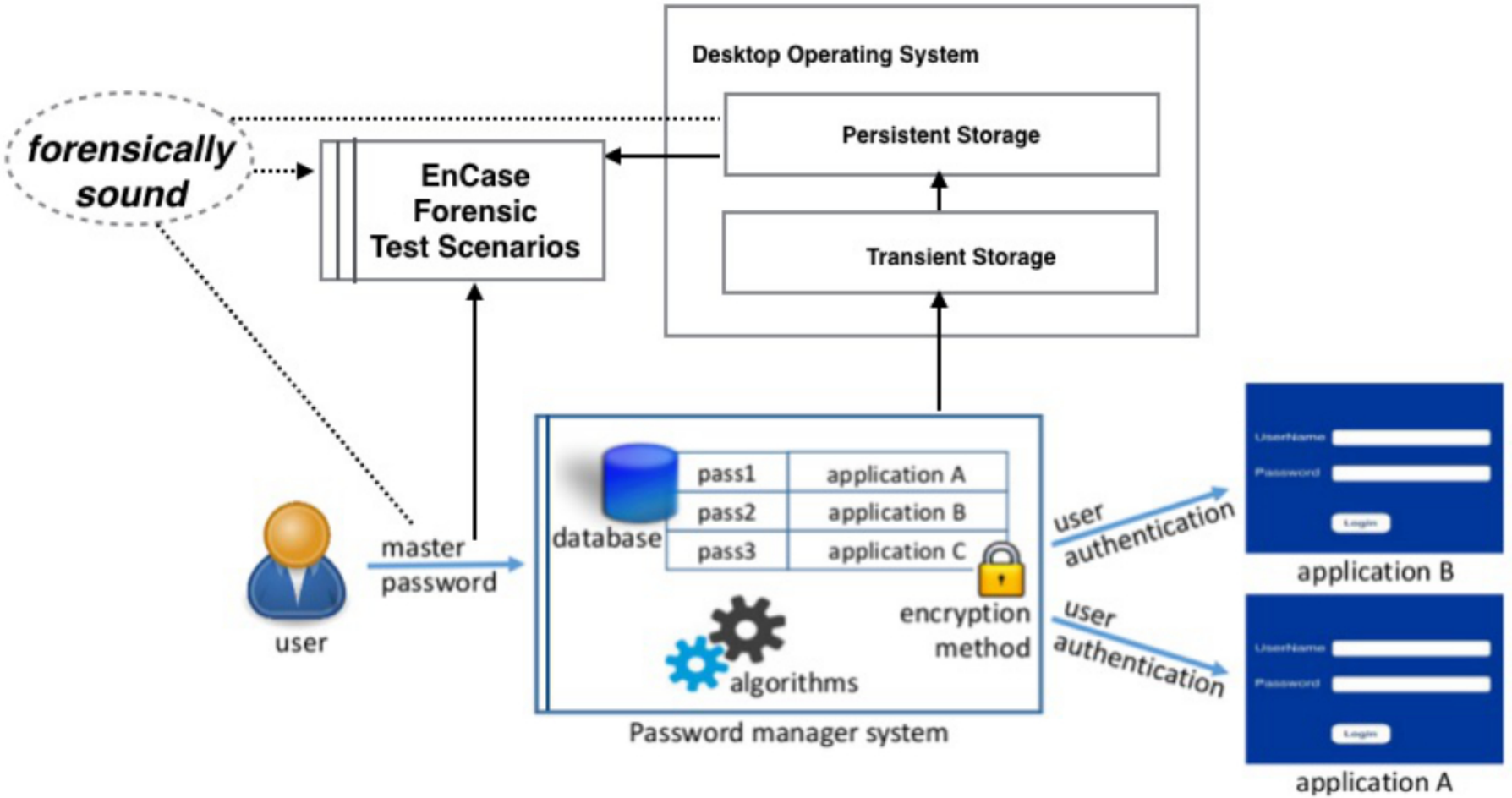
- Explores 3 popular local password managers
  - KeePass v. 2.28
  - Password Safe v. 3.35.1
  - RoboForm v. 7.9.12
- These password managers keep a database of passwords local to the machine (e.g., Windows 7) running it

Study stages

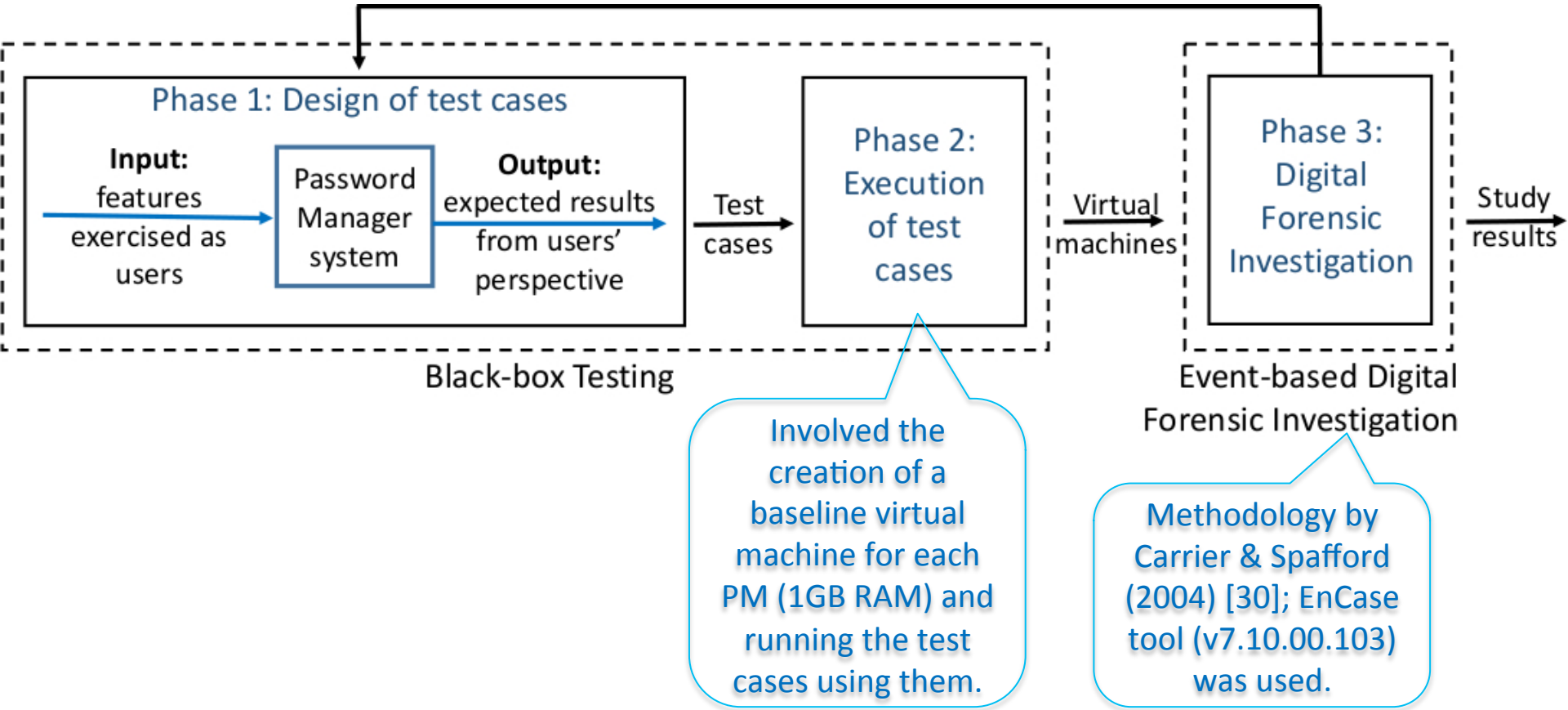
1. Elicitation of security risks & Forensic Soundness
   - Outcome: list of potential risks

2. (Forensics) phased testing approach
   - Outcome: vulnerabilities to users of the studied password managers
     – may or may not confirm the risks

Stage 1: Elicitation of security risks



Stage 2: Phased testing approach



What was tested

Password manager	Test cases	Aim
KeePass	K1-K4	Exercise methods of user authentication
	K5 & K6	Exercise export feature
	K7	Exercise print feature
	K8	Exercise uninstall feature
Password Safe	P1	Exercise methods of user authentication
	P2	Exercise export feature
	P3	Exercise clipboard feature
	P4	Exercise uninstall feature
RoboForm	R1	Exercise methods of user authentication
	R2	Exercise print feature
	R3	Exercise auto-complete feature
	R4	Exercise clipboard feature
	R5	Exercise uninstall feature

Confirmed risks via forensics: KeePass

	Expected result	Actual result (confirmed risk)
K1	Data will remain fully secured within the database.	When RAM is limited, the master password can be found in the Windows page file (hidden pagefile.sys) in plain text. (r1)
K5 K6	Despite the format, data will be exported encrypted.	No security clearance was enforced before the export started; the database exported in HTML format was unencrypted and could be easily viewed in plain text via browser; it also remained in the Recycle Bin after the user's request to permanently delete it. (r1)(r4)
K7	No residue of the failed printing will remain in the system.	No security clearance was enforced before the print started; the database print file could be located in the Temp folder in plain text after it failed to print. (r1)
K7.1	Database will print and no residue of it will remain.	The new database was deleted from the Temp folder after successfully printed; however, the unsuccessfully printed database file (see K7) remained in the Temp folder in plain text. (r1)

Confirmed risks via forensics: Password Safe (P) & RoboForm (R)

	Expected result	Actual result (confirmed risk)
P3	The copied data will be deleted from the clipboard.	The data copied to the clipboard remained stored in the Windows page file (hidden pagefile.sys) of the computer in plain text after the computer was rebooted. (r1)
R1	Data will remain fully secured within the database.	When RAM is limited, the master password can be found in the Windows page file (hidden pagefile.sys) in plain text. (r1)

Summary of risks

- With a RAM of 1GB, the master password for KeePass and identity details for payment using RoboForm can be found ***unencrypted in the page file***;
- The exported database in KeePass ***remains in the recycle bin*** even when users confirm its permanent deletion;
- Upon unsuccessful printout of KeePass database due to trivial reasons, ***the unencrypted database remains in the Temp folder*** even after closing the application, which does not happen upon successful printout;
- ***Unencrypted sensitive data copied to clipboard using Password Safe can be found in the page file*** after rebooting from a hard (non-graceful) shut down.

Discussion points

- Some vulnerabilities uncovered are bound to special conditions (e.g., paper running out, power off)
- However, they still represent risks since:
  - these conditions are likely to happen, and are sometimes trivial, and
  - malware has started to exploit password managers.

Discussion points

- Citadel (2014) malware [36] recognised the use of KeePass and Password Safe and triggered a keylogger to capture the master password
- Hacking tool KeeFarse [37] is able to dump KeePass database to a file accessible to a hacker, when a user is logged-in.
- Tools like PCT [34] can parse a live NTFS system and reconstruct a page file.
  - These show that the uncovered vulnerabilities represent *real risks*.

Conclusion (1)

- The study also allowed us to compare & contrast the behaviour of these three password managers

  Recommendations:

  1. KeePass should adopt the practice by Password Safe and RoboForm, and require security clearance in the format of authentication before processing database export and print, and
  2. Password Safe should adopt the practice by RoboForm and encrypt content copied to the clipboard.

Conclusion (2)

- Packaged as virtual machines, such test scenarios described in this work could allow regression for the improved password managers.
- Future work, e.g.:
  - Since the test cases were not exhaustive and not many features were tested, the study scope in terms of test case coverage could be extended or other systems could be examined.

References

[1] D. Florencio and C. Herley, “A Large-Scale Study of Web Password Habits,” In: Proceedings of the 16th International Conference on World Wide Web. ACM Press, 2007, pp. 657–666.

[7] A. Huth, M. Orlando, and L. Pesante, “Password Security, Protection, and Management,” United States Computer Emergency Readiness Team, 2012, https://www.us-cert.gov/security-publications/password-security-protection-and-management , last visited 10/2014.

[30] B. D. Carrier and E. H. Spafford, “An Event-Based Digital Forensic Investigation Framework,” In: Proceedings of the Fourth Digital Forensics Research Workshop, 2004, pp. 1–12.

[34] S. Lee, A. Savoldi, S. Lee, and J. Lim, “Windows Pagefile Collection and Analysis for a Live Forensics Context,” In: the Proceedings of Future Generation Communication and Networking (FGCN 2007). IEEE Press, 2007, pp. 97–101.

[36] R. Lemos, “Malware’s new target: your password manager’s password,” November 2014, visited 09/2015. [Online]. Available at: http://arstechnica.com/security/2014/11/citadel-attackers-aim-to-steal-victims-master-passwords/

[37] D. Goodin, “Hacking tool swipes encrypted credentials from password manager,” November 2015, visited 01/2016. [Online]. Available: http://arstechnica.com/security/2015/11/hacking-tool-swipes-encrypted-credentials-from-password-manager/