

Systematization of Password Manager Use Cases and Design Paradigms



James
Simmons



Oumar
Diallo



Sean
Oesch



Scott
Ruoti



THE UNIVERSITY OF
TENNESSEE
KNOXVILLE

Goal: Guide the Creation of User Studies

1. Identify understudied use cases
2. Identifying competing design paradigms that should be compared in user studies

What We Did

- Evaluated 33 password manager implementations
 - 12 desktop managers
 - 11 iOS managers
 - 10 Android managers



bitwarden



What We Did

- Extracted and prioritized use cases
 - Essential, recommended, extended
- Identified design paradigms for each use case
 - In existing tools
 - In the research literature
 - Unique to this paper
- Conducted cognitive walkthroughs as a first look at usability
 - 8 managers
 - 17 tasks covering all essential use cases

In This Talk

- Just the highlights
 - Understudied use cases
 - Gaps in the identified design paradigms
 - Interesting results from the cognitive walkthroughs

Read the paper for the full systematization and usability results

Essential Use Cases

Use Cases

(E1) Setup manager

(E2) Register credential

(E3) Update credential

(E4) Remove credential

(E5) Autofill credential

(E6) Manually enter credential

(E7) Generate password

(E8) Sync credentials

(E9) Lock manager

(E10) Unlock manager

Setup Manager

Steps

1. Find and download
2. Install
3. Set up an online account
4. Configure initial settings
5. Setup up a recovery mechanisms (rare)

Challenges

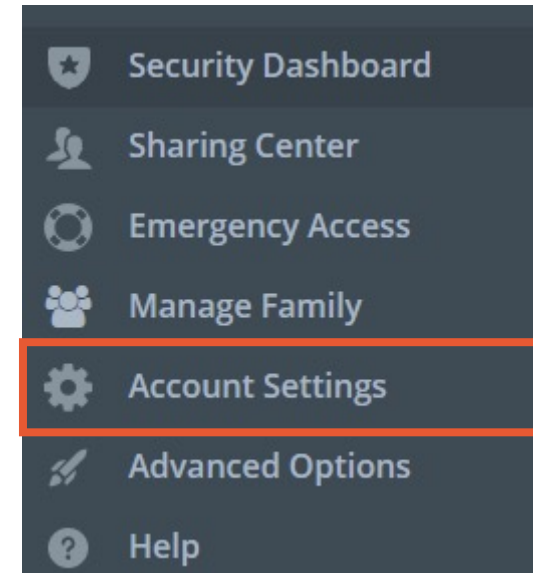
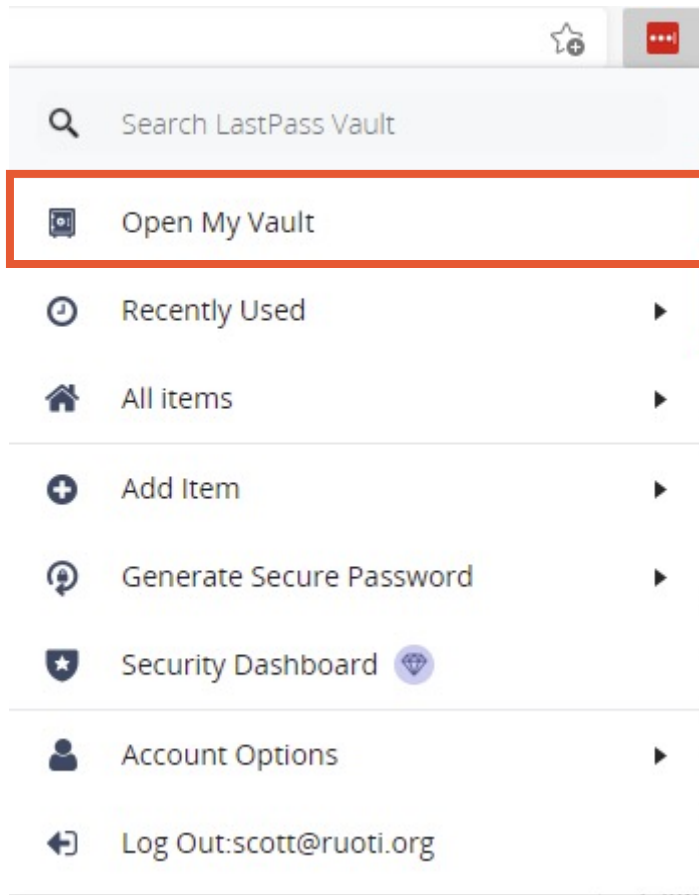
- A lot of steps, especially for non-browsers
 - Could lead to drop off if user interest is not sufficiently high
 - Makes it difficult to explore options
- Unclear what to do after setup is complete

Research is needed to smooth out the setup process

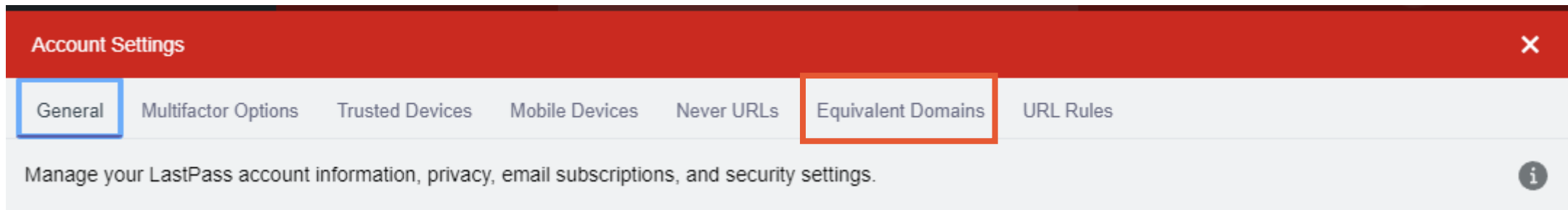
Register Credential

- Easy to register credentials
- Unless the same credential is used by two domains
 - Common authentication backend
 - Improper implementations of single sign-on
- Less than 20% of managers support credential linking
 - Poor usability
 - Leads to warnings of duplicate passwords
- Hard to use when available

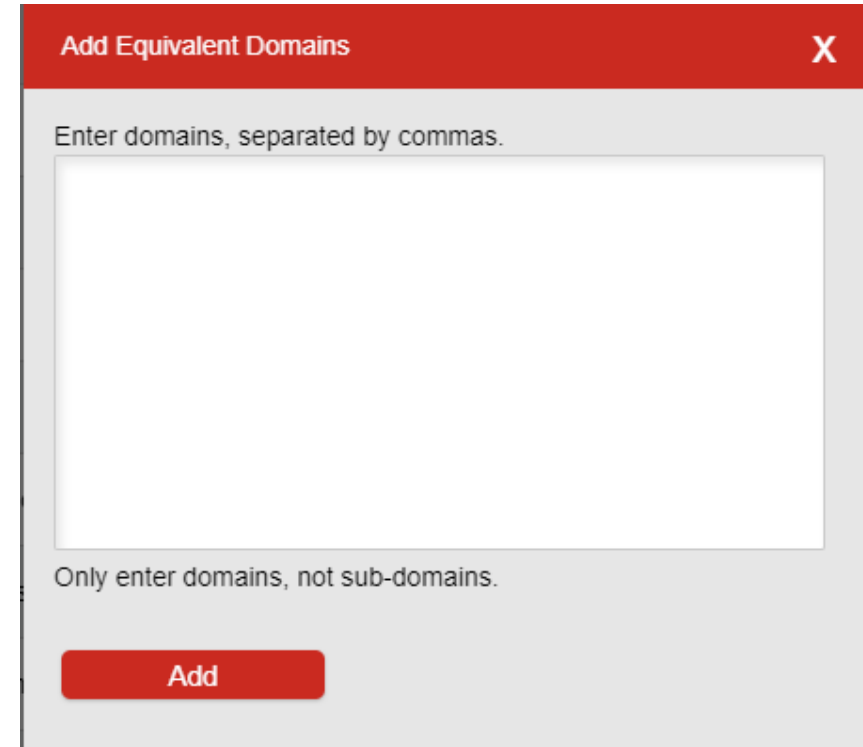
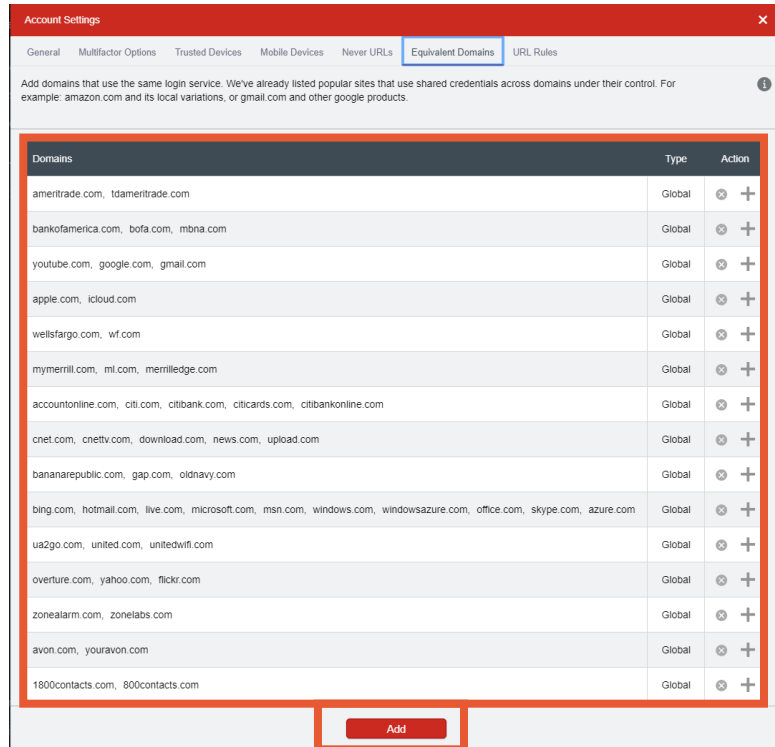
Credential Link in LastPass



Credential Link in LastPass



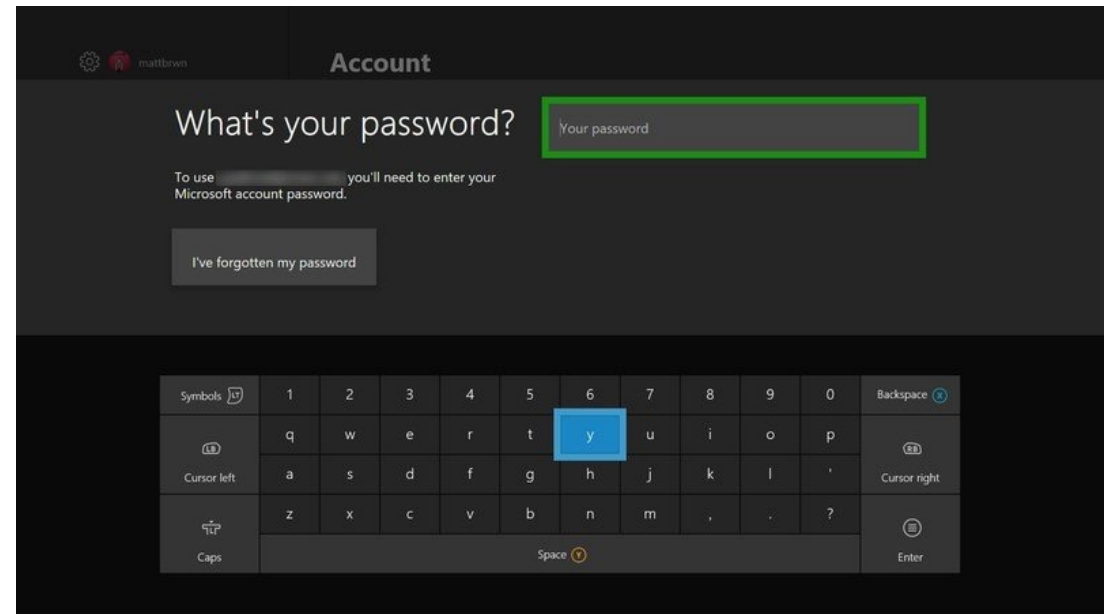
Credential Link in LastPass



Research is needed to design more usable linking paradigms

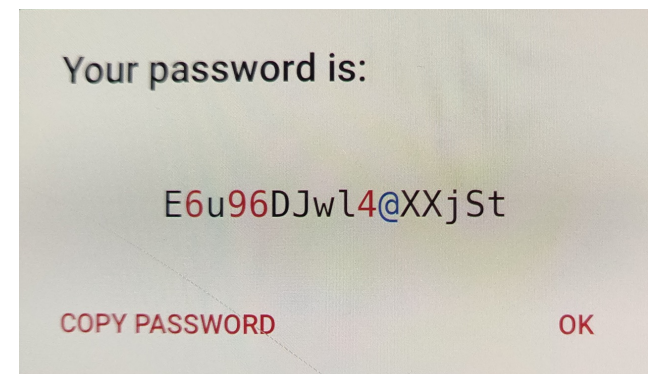
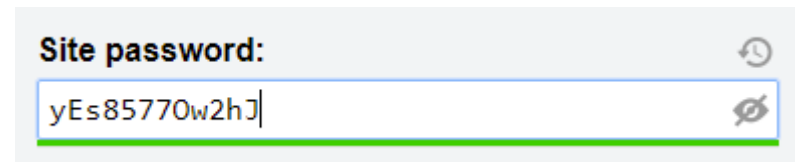
Manually Enter Credentials

- Users often need to enter credentials by hand
 - Borrowed computer
 - TV
 - Game console
 - IoT device



Manually Enter Credentials

- Entering generated credentials can be difficult
 1. Difficult to distinguish characters
 - Nearly no support on desktop
 - Some support on mobile
 2. Hard to input using the device's input method



Research is needed on modality-aware password generation

Recommended Use Cases

Use Cases

- (R1) Audit credentials
- (R2) Modify settings
- (R3) Recover access

Audit Credential

What is a credential audit?

- Evaluates the security of passwords
 - Weak passwords
 - Reused passwords
 - Compromised passwords


What are its limitations?

- Difficult to find
- Overwhelming
 - Especially on first use
- Includes false positives
- Missing design paradigms
 - Identify unused credentials
 - Prioritize recommendations

We need user studies of credential audits

Recover Access

- Losing access to a password manager is catastrophic
- Recovery mechanisms are necessary
 - Manager only as secure as the recovery mechanism
- Most managers do not have strong recovery mechanisms



1Password Emergency Kit

Created for Sherlock Holmes on July 19th, 2017.

1Password Account


SIGN-IN ADDRESS
bakerstreet.1password.com

EMAIL ADDRESS
holmes@agilebits.com

SECRET KEY
A3-FSHJNM-7T85AC-KRSBV-VC83W-7NTCN-457SS

MASTER PASSWORD

Need help?
Contact AgileBits at:
support@1password.com



Setup code
Scan this code from the 1Password apps to set up your account quickly and easily.

Research is needed on long-term recovery mechanisms

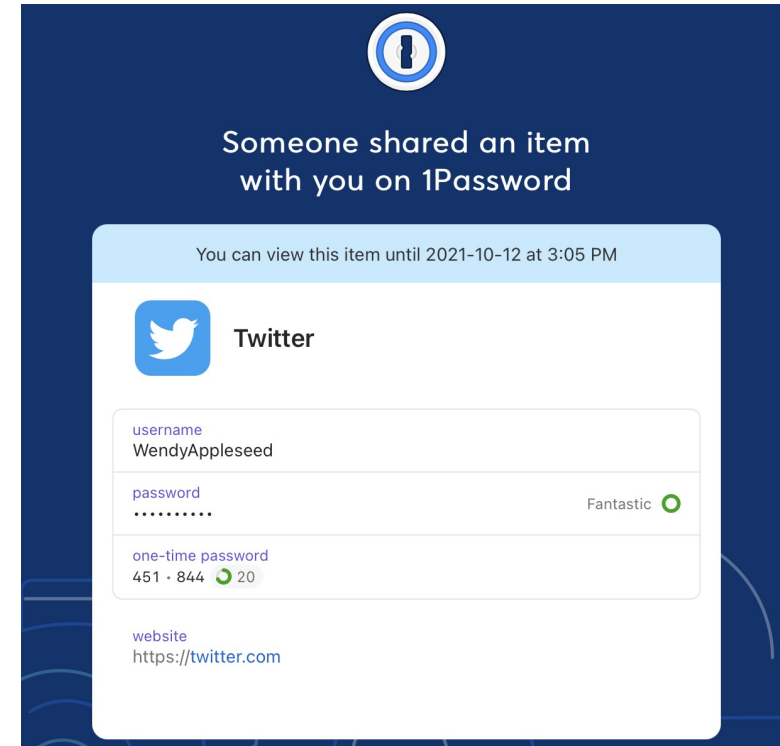
Extended Use Cases

Use Cases

- (X1) Migrate manager
- (X2) Share credentials
- (X3) Manage identities
- (X4) Store sensitive data

Share Credentials

- Sharing credentials is commonplace
 - Netflix
 - Social media
- Poorly supported
 - Between password managers
 - With non-users



We need user studies of credential sharing

Conclusion

Conclusion

- Most use cases are either unstudied or understudied
- Nearly no research has compared the strengths and weaknesses of design paradigms
- Lots of exciting research to be done in this area!

	Authors	Year	Citation	(E1)	(E2)	(E3)	(E4)	(E5)	(E6)	(E7)	(E8)	(E9)	(E10)	(R1)	(R2)	(R3)	(X1)	(X2)	(X3)	(X4)	
Security	Gasti and Rasmussen	2012	[11]																		
	Fahl et al.	2013	[9]					✓													
	Li et al.	2014	[15]					✓													
	Silver et al.	2014	[30]					✓													
	Stock and Johns	2014	[32]					✓													
	Oesch and Ruoti	2020	[19]					✓		✓											
Oesch et al.	2021	[18]					✓														✓
Interview	Fagan et al.	2017	[8]		✓																
	Pearman et al.	2019	[21]		✓																
	Ray et al.	2021	[22]		✓																
Usability	Lyastani et al.	2017	[16]		✓	✓					✓										
	Seiler-Hwang et al.	2019	[29]	✓	✓	✓									✓						
	Huaman et al.	2021	[13]		✓	✓															
	Chiasson et al.	2006	[3]		✓	✓				✓											
McCarney et al.	2012	[17]		✓	✓																
Stobert et al.	2020	[31]		✓	✓		✓														

Table 3: Use cases examined in prior usability studies

Our systematization is aimed to help jump start this research

