ACSAC 2024

南開大學
Nankai University

Leaky Autofill: An Empirical Study on the Privacy Threat of Password Managers' Autofill Functionality

---

Yanduo Fu and Ding Wang*

College of Cyber Science, Nankai University, Tianjin, China

December 11, 2024

Passwords suffer from usability-security dilemma

Increasing account numbers

80-112 accounts[1-2] before COVID-19

↓

168 accounts[3] after COVID-19

Password guidelines

Creating **random & unique** passwords for each account

↓

Enhancing password security for web users

Heavy management burden!

Using **popular or similar** passwords across multiple accounts

↓

Passwords are reused and guessable

[1] Leveraging semantic transformation to investigate password habits and their causes. In Proc. CHI 2018, pp. 1-12.
[2] Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat. In Proc. ACM CCS 2017, pp. 295-310.
[3] Juggling security: How many passwords does the average person have in 2024? https://nordpass.com/blog/how-many-passwords-does-average-person-have/

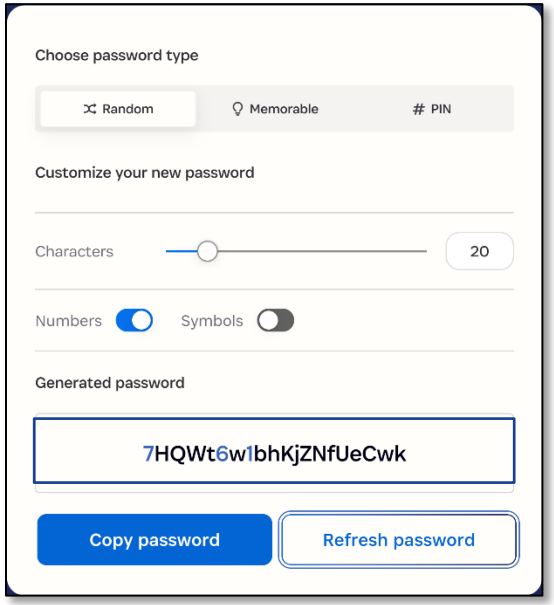
Password managers provide a technical solution

Built-in-browser PMs

LastPass
bitwarden
RoboForm
Sticky Password
securing your personal data
1Password
KEEPER
kaspersky
AVIRA
True Key
Proton Pass
DASHLANE
PASSWORD BOSS
norton

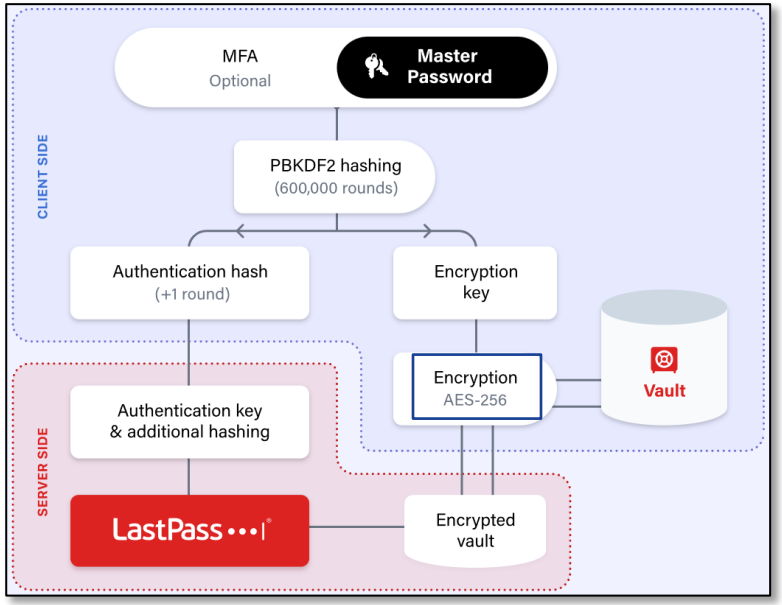
Separately-installed PMs

Password managers provide a technical solution



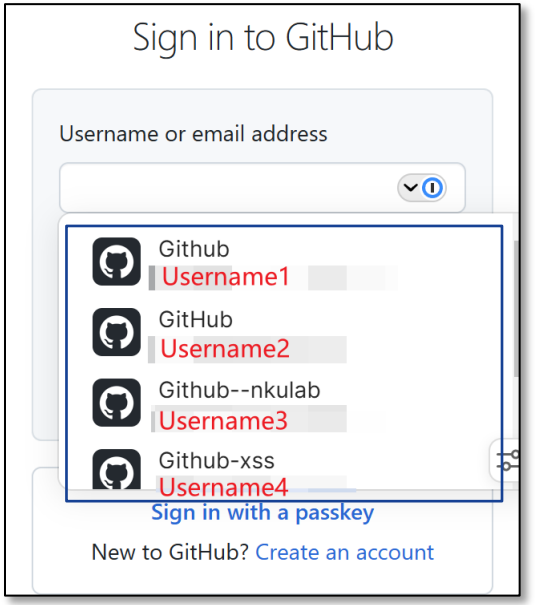
[1Password]

Generate strong passwords



[LastPass]

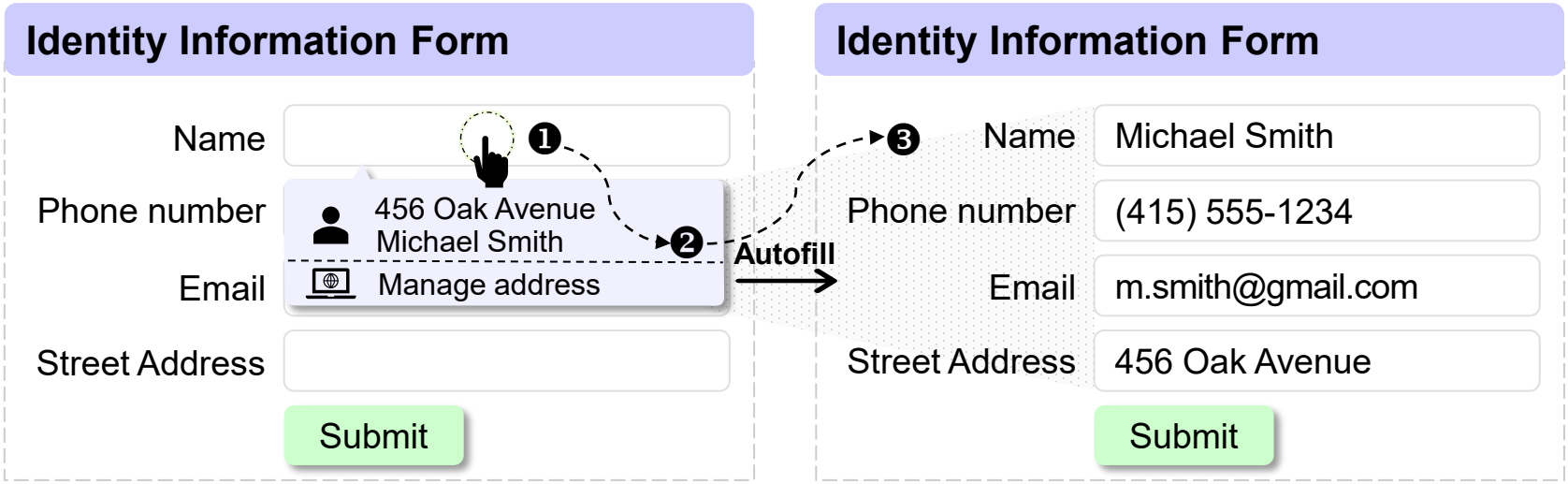
Encrypted storage



[1Password and GitHub]

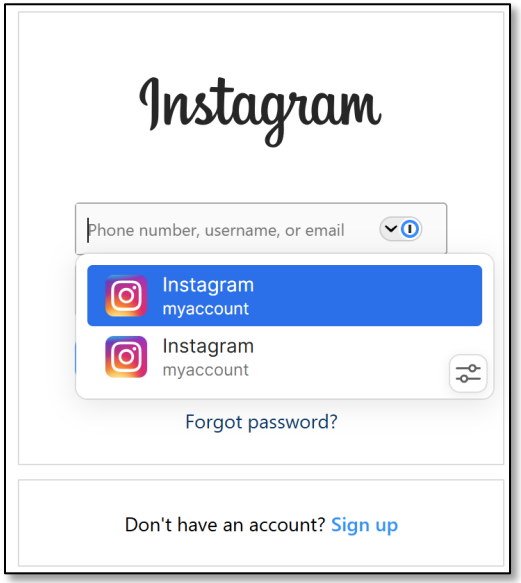
Convenient autofill

Introduction to the autofill functionality

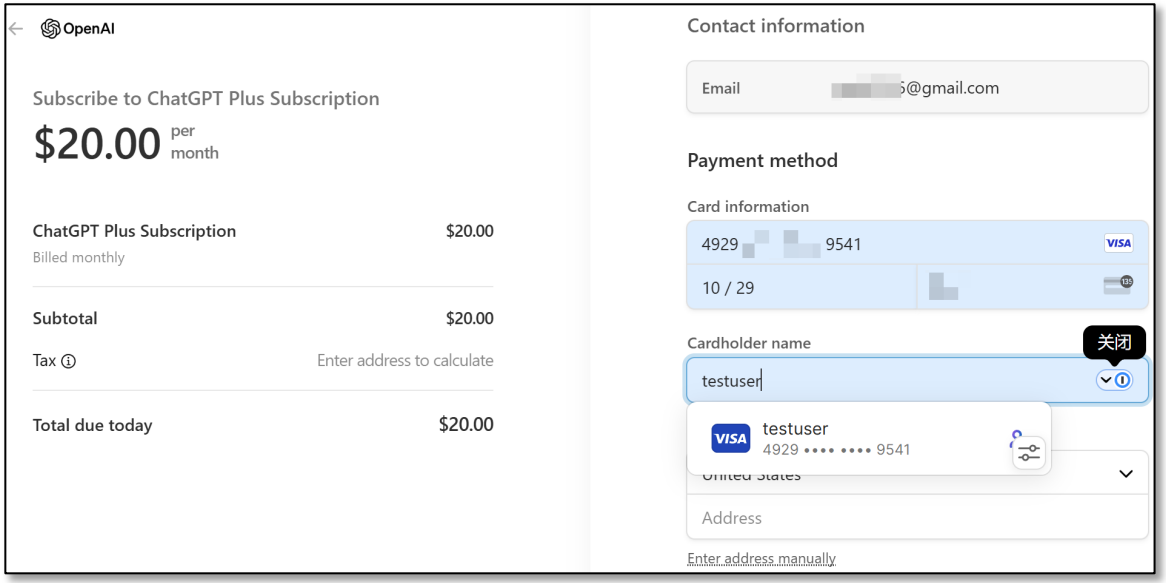


Users only need **one or a few** click(s) to fill in the web form with the autofill functionality

Introduction to the autofill functionality



[1Password and Instagram]

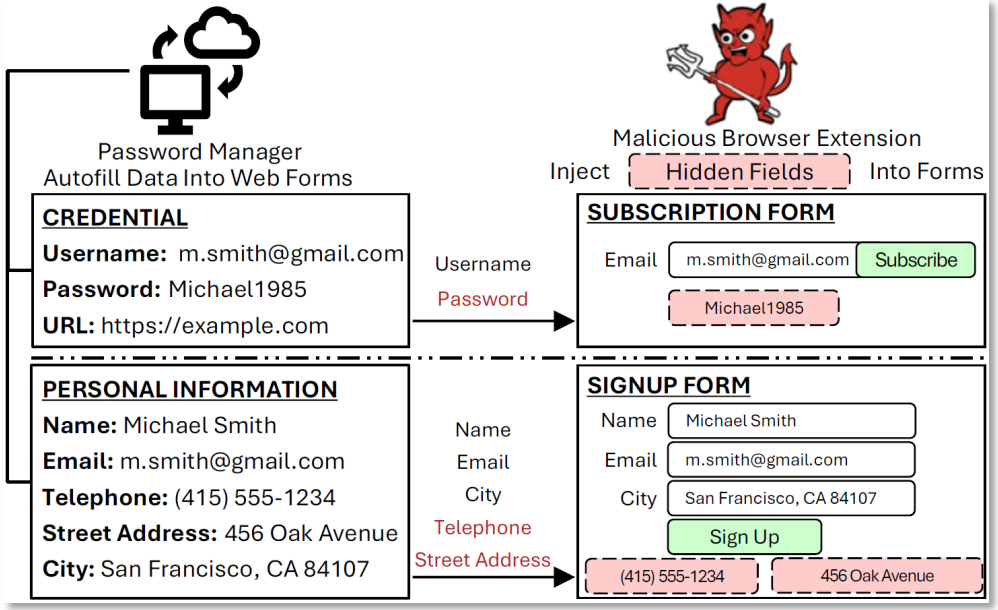


[1Password and Open AI]

Users only need **one or a few** click(s) to fill in the web form with the autofill functionality

Problem statement

An attack example



Threat model

The attacker could:

(1) … inject **invisible** <input> elements into web forms, e.g., password, address

(2) … wait for the user triggering the autofill functionality to fill in stored data

(3) … retrieve the filled **sensitive** data without users' **knowledge** or **consent**

Type of attackers:

(1) Malicious browser extensions

(2) Curiosity-driven websites

Our work

Previous research

Source	Target Object	Concealment Techniques
ACM CCS'20[4]	Six built-in-browser PMs	Eight concealment techniques
PETS'20[5]	Only Firefox browser	Not specified
ASIACCS'14[6]	Six built-in-browser PMs	Only `hidden`

- Only built-in-browser password managers
- Limited concealment techniques
- **A question arises:**

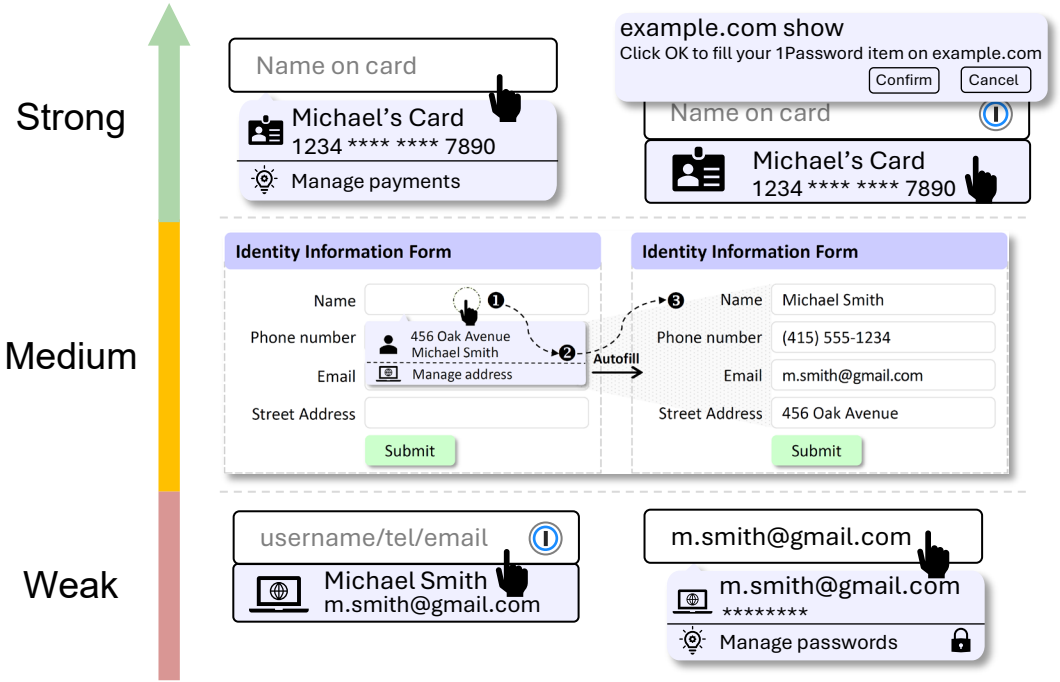
How do perceived more secure **separately-installed password managers** perform on identifying invisible fields on web forms?

Overview of our work

- **30** password managers, including **24** separately-installed and **six** built-in-browser password managers
- **15** concealment techniques for web form fields, with **seven** newly considered techniques, such as `clip`, `clip-path`, `transform`, `content-visibility`, …
- **Three** kinds of web forms:
  - Identity information form
  - Credit card form
  - Login form

[4] Fill in the Blanks: Empirical Analysis of the Privacy Threats of Browser Form Autofill. In Proc. ACM CCS 2018, pp. 507-519.
[5] No boundaries: data exfiltration by third parties embedded on web pages. In Proc. PETS, pp. 295-310.
[6] Protecting Users Against XSS-based Password Manager Abuse. In Proc. AsiaCCS, pp. 183-194.

RQ1: User interaction strength of the autofill functionality - Intro



Strong user interaction strength

- Detailed information of filled data and form
- Warnings or re-authentication for users

Medium user interaction strength

- Require **user interaction** to trigger the autofill functionality, yet provide **unclear** information about the filled data type

Weak user interaction strength

- Provide nothing about form and data type
- Autofill on page loading

RQ1: User interaction strength of the autofill functionality - Result

TABLE 1: Selected password managers, default autofill behaviors, and the interaction strength*.

Name	Info†	Version	Personal Info				Credit Card				Login			
			Method‡	Detail	Prompt	Level♭	Method	Detail	Prompt	Level	Method	Detail	Prompt	Level
LastPass: Free Password Manager	10,000k	4.130.2.1	ClickIcon	◇	Warn	S	ClickIcon	✓	Warn	S	On load	✓	⊘	W
Avira Password Manager	6,162k	2.20.0.4570	-	-	-	-	-	-	-	-	On load	✓	⊘	W
Norton Password Manager	5,194k	8.2.0.161	-	-	-	-	ClickIcon	✓	⊘	S	ClickIcon	✓	⊘	S
1Password – Password Manager	4,443k	2.23.3	ClickIcon	×	⊘	W	ClickIcon	✓	Warn	S	ClickIcon	×	⊘	W
Bitwarden - Free Password Manager	3,903k	2024.4.1	RightClick	◇	⊘	M	RightClick	✓	⊘	S	ClickIcon	×	⊘	W
Kaspersky Password Manager	2,385k	24.0.128.1	ClickIcon[1]	✓	⊘	S	ClickIcon[1]	✓	Warn	S	On load	×	⊘	W
Dashlane — Password Manager	2,194k	6.2418.0	ClickIcon	◇	⊘	M	ClickIcon	✓	Mpw	S	On load	✓	⊘	W
iCloud Passwords	2,035k	2.2.9	-	-	-	-	-	-	-	-	ClickIcon	✓	⊘	S
Keeper Password Manager & Digital Vault	1,343k	16.8.3	RightClick	◇	Warn	S	RightClick	✓	Warn	S	ClickIcon	✓	⊘	S
MultiPassword — Password manager	1,288k	0.97.4	-	-	-	-	-	-	-	-	ClickIcon	×	⊘	W
True Key by McAfee	801k	4.3.1.9339	-	-	-	-	-	-	-	-	On load	×	⊘	W
RoboForm Password Manager	665k	9.5.9.2	ClickIcon	◇	⊘	M	ClickIcon	✓	⊘	S	ClickIcon	✓	⊘	S
DualSafe Password Manager & Digital Vault	494k	1.4.28	-	-	-	-	-	-	-	-	On load	×	⊘	W
NordPass (desktop app version)	460k	5.15.28	ClickIcon	◇	⊘	M	ClickIcon[1]	✓	⊘	S	ClickIcon	✓	⊘	S
ExpressVPN Keys: Password Manager	391k	2.0.12.715	-	-	-	-	ClickIcon	✓	⊘	S	ClickIcon	×	⊘	W
Dropbox Passwords	374k	3.26.0	-	-	-	-	ClickIcon	✓	⊘	S	On load	✓	⊘	W
KeePassXC-Browser	369k	1.9.0.4	-	-	-	-	-	-	-	-	ClickIcon	×	Warn	S
NordPass Password Manager & Digital Vault	239k	5.15.29	ClickIcon	◇	⊘	M	ClickIcon[1]	✓	⊘	S	ClickIcon	✓	⊘	S
Passbolt - Open source password manager	233k	4.7.7	-	-	-	-	-	-	-	-	ClickIcon	✓	Mpw	S
Proton Pass: Free Password Manager	210k	1.14.1	-	-	-	-	-	-	-	-	ClickIcon	✓	⊘	S
Microsoft Autofill	140k	2.0.5	ClickIcon	✓	⊘	S	ClickIcon	✓	⊘	S	ClickIcon	✓	⊘	S
Zoho Vault	134k	4.0	-	-	-	-	ClickIcon	✓	⊘	S	ClickIcon	✓	⊘	S
Enpass Password Manager	124k	6.9.3	RightClick	◇	⊘	M	ClickIcon	✓	⊘	S	ClickIcon	×	⊘	W
Password Manager SafeInCloud	107k	24.1.0	-	-	-	-	Extension	✓	⊘	S	Extension	×	⊘	W
Google Chrome	65.38%	124.0.6367.119	ClickIcon	◇	⊘	M	ClickIcon	✓	⊘	S	On load	✓	⊘	W
Microsoft Edge	12.75%	123.0.2420.81	ClickIcon	✓	⊘	S	ClickIcon	✓	⊘	S	On load	✓	⊘	W
Safari	8.72%	17.3.1	ClickIcon	✓	⊘	S	ClickIcon	✓	⊘	S	ClickIcon	✓	⊘	S
Mozilla Firefox	7.26%	125.0.3	ClickIcon	✓	⊘	S	ClickIcon	✓	⊘	S	ClickIcon	✓	⊘	S
Opera	3.05%	109.0.5097.80	ClickIcon	◇	⊘	M	ClickIcon	✓	⊘	S	On load	✓	⊘	W
Brave	-	1.65.130	ClickIcon	◇	⊘	M	ClickIcon	✓	⊘	S	ClickIcon	✓	⊘	S

* '-': Not applicable due to not being autofillable; ✓: Clear indication of filled form and data type; ◇: Only indication of filled form type; ×: No indication of what form and data will be filled; 'Warn': Warning dialog pops up before filling the form; 'Mpw':Master password required before filling the form; ⊘: No warnings shown, or permission and re-authentication required.
† Active users of Chrome browser extensions for 24 separately-installed PMs from ChromeStats [11] and market share of six browsers with built-in PMs sourced from StatCounter [56].
‡ Autofill triggering method. 'On load' means that the information is filled into the fields when the web page loads; 'ClickIcon' means users need to click the PM icon in the web form field or click the field to trigger the autofill functionality; 'ClickIcon[1]' means that the PM icon only appears in the *targeted sensitive* field; 'RightClick' means that users need to right-click the web page to select the PM menu to trigger the autofill functionality; 'Extension' means that users need to click the extension in the browser menu bar to trigger the autofill functionality.
♭ **W** means the PM has **W**eak user interaction strength for autofill functionality in this form, **M** for **M**edium interaction strength, and **S** for **S**trong interaction strength.

30 PMs autofill **69** scenarios

17 for personal information forms

- **10** PMs provide little information about filled data and form type

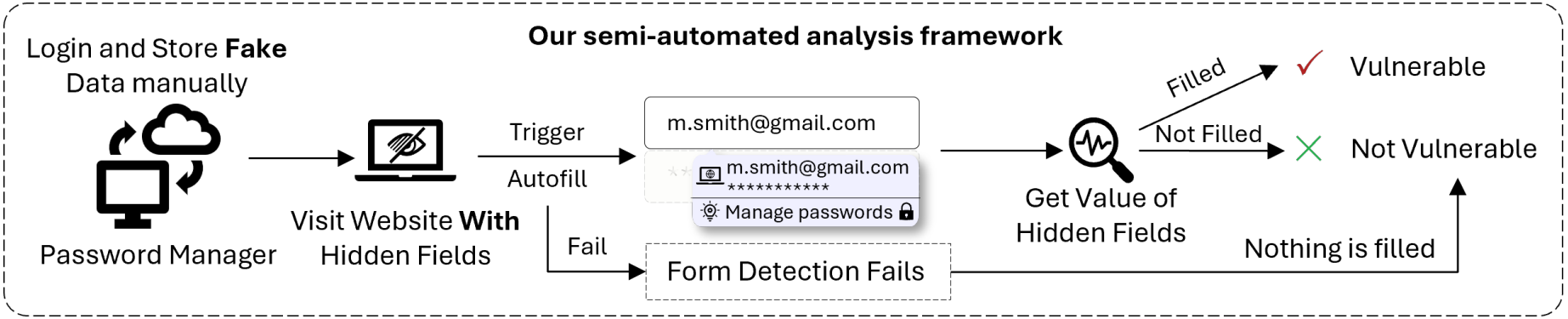
22 for credit card forms

- All PMs provide **strong** interaction

30 for login forms

- **16** PMs provide weak interaction
- **10** PMs autofill on page loading

RQ2: The ability in detecting hidden form fields - Method

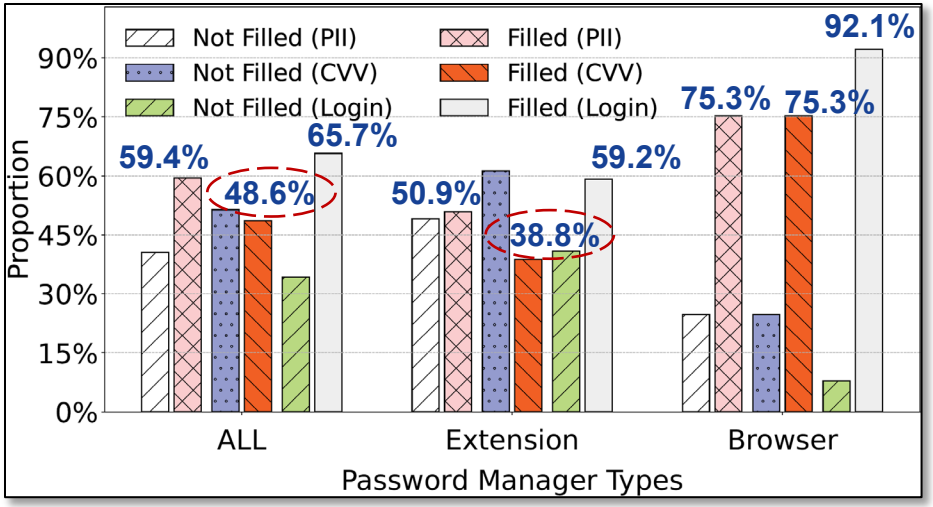


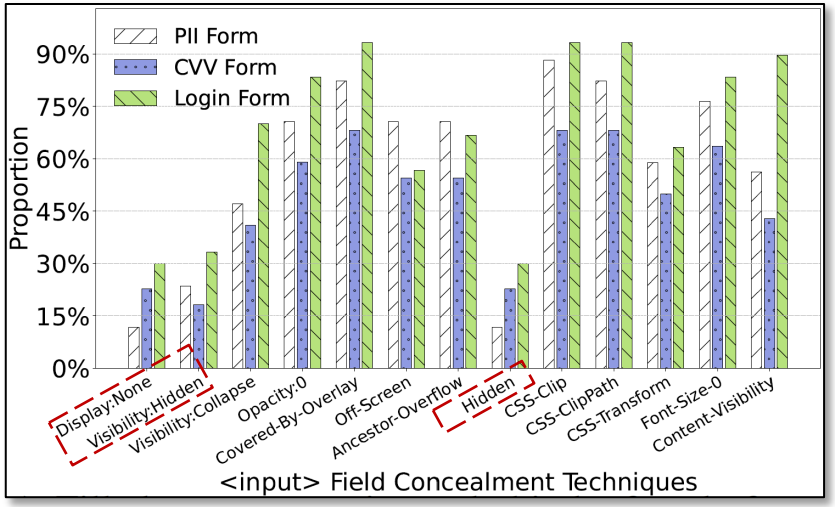
1. Start a browser instance and log into the password manager account
2. Import/Add test data into password manager for each web form
3. Access the test website and trigger the autofill functionality using Selenium
4. Using Selenium to log which data gets auto-filled

Require **one-time** human operation

Automated testing and logging using Selenium

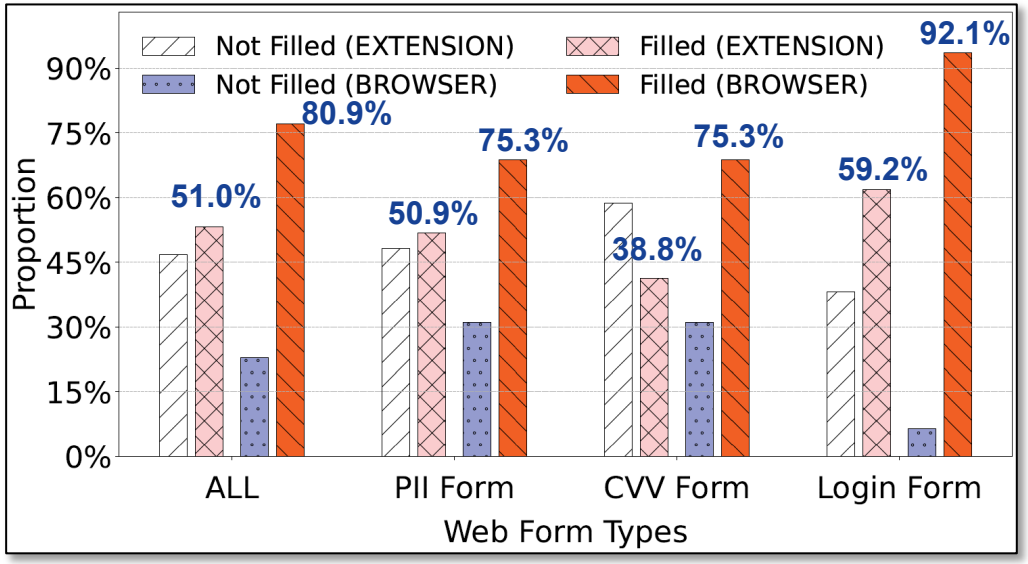
RQ2: The ability in detecting hidden form fields - Result





- Filled probability of **credit card forms** is **48.6%**, where **38.8%** for separately-installed PMs
- Hidden fields in **credit card forms** are significantly less likely (**0.494 times**) to be filled than **login forms**
- **83.3% (25/30)** PMs successfully detect **three techniques** in at least one web form

RQ3: Comparison between two kinds of password managers



- Built-in-browser PMs are more likely **(~4.07 times)** to fill data into hidden fields than separately-installed PMs
- No obvious improvements for built-in-browser PMs

Concealment Tech.†	Display: None	Visibility: Hidden	Visibility: Collapse	Opacity: 0	Covered by Overlay	Non-Effective-Size	Off-Screen	Ancestor-Overflow	Hidden	CSS Clip	CSS Clip-Path	CSS Transform	Font Size: 0	Content-Visibility	Tiny-Size
Chrome	×	×	×	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓
Edge	×	×	×	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓
Safari	×	×	×	✓	✓	×	✓	✓	×	✓	✓	✓	✓	-[1]	×
Firefox	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Opera	×	×	×	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓
Brave	×	×	×	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓

Table 1: Browsers that autofill form fields that are hidden from the user, based on various concealment techniques.

Techniques	Firefox	Chrome	Brave	Edge	Safari	Opera
CSS Display	✓	✗	✗	✗	✗	✗
CSS Visibility	✓	✗	✗	✗	✗	✗
CSS Opacity	✓	✓	✓	✓	✓	✓
Covered by overlay	✓	✓	✓	✓	✓	✓
Non-effective size	✓	✓	✓	✓	✓	✓
Off-screen placement	✓	✓	✓	✓	✓	✓
Ancestor's overflow	✓	✓	✓	✓	✓	✓

[From ACM CCS'20[4]]

[4] Fill in the Blanks: Empirical Analysis of the Privacy Threats of Browser Form Autofill. In Proc. ACM CCS 2018, pp. 507-519.

Issues report and countermeasures

Reporting privacy threats to password vendors

LastPass → **Confirmed** but not solved

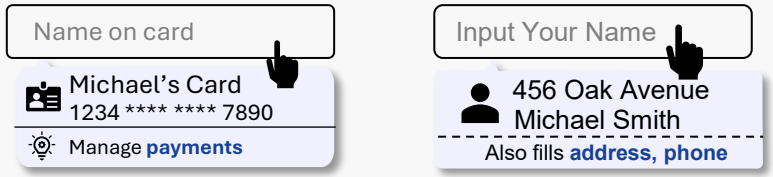
1Password → A compromised client-side is **not** considered

bitwarden, KeePassXC → Consider the **balance** between user experience, performance, and security

Two suggestions to reduce privacy threats

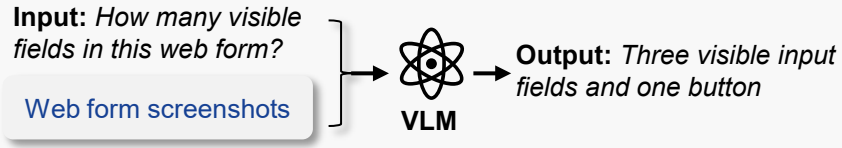
1. Increasing user interaction strength

- Prevent autofill on page loading
- Specifying the type of filled data and type



2. Using visual language model

- Counting and filling visible form fields



Thank you!

Leaky Autofill: An Empirical Study on the Privacy Threat of Password Managers' Autofill Functionality

Yanduo Fu and Ding Wang*, Nankai University

https://zenodo.org/records/13380735

https://github.com/Leaky-Autofill

https://leakyautofill.github.io/

wangding@nankai.edu.cn

- An empirical study on the privacy threat of the **autofill functionality** of 30 password managers
- A **semi-automated** password manager autofill functionality end-to-end testing tool

More research about identity authentication security, see https://wangdingg.weebly.com/publications.html