Supplementary Material – *"I have no idea how to make it safer"*: Studying Security and Privacy Mindsets of Browser Extension Developers

Anonymous

A Pilot study

A.1 General outline

To be able to validate and verify the feasibility of our methods, we conducted a total of five pilot interviews before recruiting the actual extension developers. All five participants (*PS1 – PS5*) had backgrounds in computer science and Cybersecurity, with familiarity in Web development. Although they had developed at least one extension, none had published them on Web stores, using them only for personal or research purposes.

In the coding task phase of the interview, we asked each participant to work on two coding tasks. We initially started this phase with *CT3* (see detailed description below), a third coding task that was attempted by *PS1*, *PS2*, and *PS3*, and that was followed by *CT1*. During this exercise, we observed that *CT3* required substantial background knowledge and effort from participants, making it infeasible under the time and environmental constraints of the interview (refer to Table 1 for more details). As a result, we replaced *CT3* with *CT2* and proceeded to use *CT1* and *CT2* as the primary tasks, reserving *CT3* as an optional task for high-performing developers.

The pilot tests enabled us to refine the coding tasks by adding comments and improving task instructions to reduce unnecessary cognitive burden for participants. Lastly, the pilot study confirmed the validity and applicability of the interview questions, with minor adjustments to framing and order. Notably, the data collected during the pilot tests were not used in the final analysis, and we do not report the results of *CT3* in this paper as only two developers attempted the task.

Participants	Coding Tasks		
	CT1	*CT2*	*CT3*
PS1	●	–	⊕
PS2	⊕	–	⊘
PS3	–	⊗	⊘
PS4	–	●	●
PS5	–	●	●

Table 1: The pilot study participants worked on two coding tasks and the above table outlines the status of the individual tasks (● : Completed, ⊘ : Did not finish, ⊕ : Did not finish, but outlined approach).

A.2 Coding Task 3

Hausknecht et al. [2], and more recently Agarwal [1], reported that the `Content-Security-Policy` along with the `X-Frame-Options` headers are the most popularly targeted security headers that extension modify for their functionality. Considering this, we also designed a third coding task that required the extension developers to modify the existing CSP of the test website, which only allowed scripts from the same origin. Specifically, the developers were asked to inject a third-party code snippet to the page through the extension which, then, included further script and added a *Share on Facebook* button to the product page for each of the listed products [3]. Through this task, we wanted to capture their working knowledge of security primitives, such as CSP, and their mindset when handling issues that require changing the security configurations on the client side for their functionality. In this case, they needed to modify the existing CSP to allow-list `*.facebook.net` domain. The security-focused solution would require developers to include the domain to be allow-listed under the `script-src-elem` directive; thus, any future changes to the `script-src` directive would not break the extensions' or the websites' functionality.

While the solution strategy is similar to that of *CT2*, we realized during the course of the study that - a.) not many people have the working knowledge of CSP, and b.) the task was too complicated to be solved within a reasonable amount of time and interview setting. Further, due to time constraints, we only offered the participants to work on this task as an optional component of the interview, and also based on the time taken to solve the other two tasks. Thus, only two participants (*P03, P04*) opted to solve the task, and we decided to exclude this from our analysis due to lack of data points

for comparison. Interestingly, both participants successfully solved the task and were reluctant to publish extensions that dropped the CSP header entirely due to security reasons. They modified the existing header and the `script-src` directive to allow-list the required domain. Additionally, *P03* also explained that the solution is brittle and will break the website in the future if the original CSP configuration changes but the extension does not incorporate them. However, they are not aware of any other alternatives.

B Pre-Screening Questionnaire

1. How many years of experience do you have working with extension development?
2. Select all the categories that apply to browser extensions you have published in any of the extension stores:
3. What is / are the motivating factor(s) that drives you to develop browser extensions? (Select all that applies)
4. Did you study computer science:
   - at an undergraduate level.
   - at an graduate level.
   - via professional training.
   - in high school.
   - did not study.
   - others.
5. Are you currently working in the area of computer science, engineering or Web development?
6. Do you have experience working with other Web Technologies?
7. What is your age in years?
8. What is your gender?
9. What is your nationality?

10.1. Please enter your email address here:

10.2. If you would like to be contacted for the online interview on a different email address, please enter the new email address here:

C Inclusion of Participants with Low Installs

As reported in Table 2 of the original paper, four of our participants (*P02*, *P05*, *P09*, *P10*) less than 100 install counts in total. While the S&P mindset of extension developers with low install counts may incur potential bias, however, we included the observations from these participants since they showed apparent signs of S&P mindset during the course of the interview. We detail individual cases and our assessment for them in the following:

- *P02* elaborated on the design and development steps of one of their "bigger" work-in-progress extension projects, which would handle users' authentication details and their S&P in the same way they do for the current extension – *"...if you are like taking more permissions like if you want access to background tabs right then you also have to provide a detailed description on why you need this permission right and if you're collecting some data right so you have to provide them why specifically you need this data, right?"*.
- *P05* recently published a B2B product with monetary incentives for bot detection purposes. They also explicitly mentioned that they learned security and privacy practices and consulted IT lawyers for advice on complying with different privacy regulations worldwide – *"...I read about how dangerous extensions can be, ...and so many are used to steal your data. So many are used to steal your passwords."*.
- *P09* explained that their extension performed content filtering and moderation on social media feeds, and thus, it was necessary for them to handle the feed data associated with individual users in a privacy-friendly manner – *"...And there are all sorts of security implications and like privacy concerns when, if you'd have to like take it on a broader space for other people."*.
- *P10* explained that their extension performs sensitive operations on a small set of banking sites and mentioned that their extension must have privacy mechanisms in place. Additionally, they are an active member of the Mozilla Add-Ons Content Review Team. They reviewed the S&P of submitted extensions, among other aspects, and provided guidance to other extension developers, thus acting as a multiplier of S&P knowledge within a broader extension-developer community – *"...At the top of my mind is privacy. I am very much concerned that you should not breach the user's privacy."* / *"...I was one of the panelists in the Add-Ons Review Committee for Recommended Badges, along with three Mozilla employees."*

D Axial Categories for Coding Tasks

1. Status quo (what an interviewee knew about the problem underlying the respective coding task based on his or her previous experience).
2. Familiarity with the coding task.
3. Path of actions (whether a developer followed a linear path of actions, took some detours, or even radically changed their path after realizing that the initially chosen one is a dead-end street).
4. Explicit statements or actions demonstrating their understanding of the respective coding task.
5. External sources of knowledge used during the development process.

6. Critical junctures, i.e., situations where the interviewee had to make crucial decisions.
7. Statements or actions demonstrating developer's S&P awareness.
8. End Strategy.
9. S&P assessment of the end strategy.
10. Detection of over-permissions.

E Additional Listings, Figures and Tables

Categories	Motivation
Functionality & UI, **Tools (including search tools)**, **Accessibility**, **Workflow & Planning**, Appearance, Education, Entertainment, Communication, **Social Networking**, **Just for Fun**, **Bookmarks**, **Tabs**, Alert & Updates, **Photos/Music/Videos**, Art & Design, **Search Tools**, **Developer Tools (including Web development tools)**, **Well-being**, **Privacy & Security**, **Language Support**, **Feeds/News/Blogs**, Shopping, News & Weather, Games, **Downloads Management**, Household, *Productivity*, *Business/SaaS*, *Automation*, *Archiving*, *Intelligence*	**Leisure/fun**, **Business (Self)**, **Additional monetary benefits (e.g. through ads etc.)**, **Utility (For personal or community use)**, **Business (Employer)**, **Testing other applications**, *Personal Interest*, *Tool Creation*, *Education Focus*, *Problem Solving*, *Toy Project*, *Learning Experience*, *University Project*, *Control the influence of Google Search Engine*, *Selfless Sharing*, *Information Reduction*, *Customization*, ***Employment***, *Browser Insight*, *Personal Achievement*, *Curiosity Driven*, *Ad Blocker*, *Front-end Study*, *Social Change*

Table 2: The extension categories and the motivation to develop and publish extensions reported by all the 165 people who finished the pre-screening survey. The *italicized* items are provided by people in the free text field while the **bold** items are also reported by the interview participants.

```
async function recordAddressData(addressData) {
    try {
        console.log("Address Data:", addressData);
        // do something here.
    } catch (e) {
        console.error(e);
    }
}

async function retrieveAddress() {
    try {
        // do something here.
    } catch (e) {
        console.error(e);
    }
}
```

Listing 1: CT1: The code blocks to be implemented.

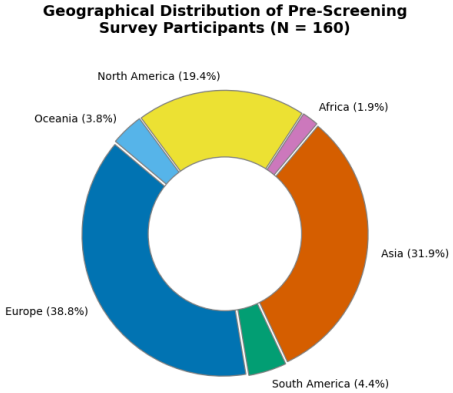

Figure 1: The continent-wise distribution of developers who finished the pre-screening survey and provided consent to participate in the study. 5 people did not provide any response.

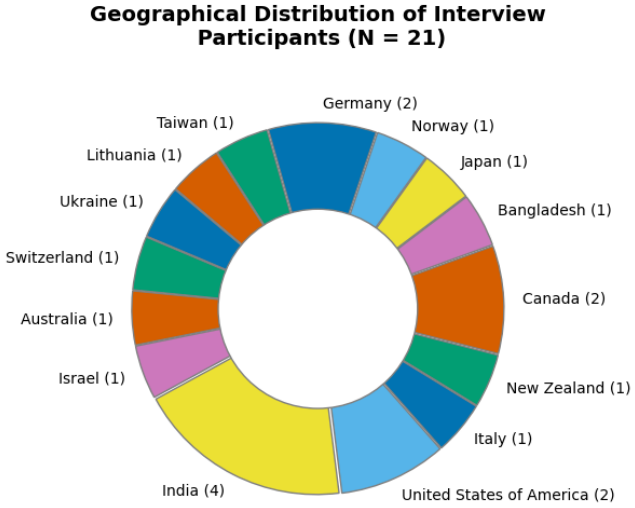

Figure 2: Country-wise distribution of study participants.

References

[1] Shubham Agarwal. Helping or Hindering? How Browser Extensions Undermine Security. In *CCS*, 2022.

[2] Daniel Hausknecht, Jonas Magazinius, and Andrei Sabelfeld. May i?-content security policy endorsement for browser extensions. In *DIMVA*, 2015.

[3] Meta. Share button, 2025. URL https://developers.facebook.com/docs/plugins/share-button/.