User Survey on Malicious MCP Servers - Interview Section

Thank you very much for taking the time to participate in this interview. The purpose of this interview is to gain a deeper understanding of your experiences and thoughts while completing the previous user research tasks, so that we can better understand users' security awareness and needs in the MCP ecosystem.

Part One: Task Review

1. During Task One, when you were browsing the simulated website and "installing" servers, did any servers raise your suspicion and make you feel they might be malicious? If so, which servers? What specific aspects (e.g., description, name, functionality, source code snippets, etc.) made you find them suspicious? (This refers to whether users could recognize malicious servers during Task One)
2. During the process of browsing MCP servers on the simulated website in Task Two, how confident were you in your ability to identify potentially malicious MCP servers?
3. During Tasks Two and Three, if you discovered malicious MCP servers, how did you determine that these MCP servers were malicious? In this analysis process, which of the three types of information - "introduction and description information," "source code," and "configuration methods" - did you find most useful for judging malicious behavior? Which was least useful or most difficult to utilize? Why?
4. While reviewing the source code, were there any specific code patterns, function calls, or data processing methods that particularly raised your alarm? Or, were there any parts that you found difficult to understand but felt might pose risks?
5. *[Explain to the interviewee the four attack types and methods of malicious MCP servers].* How do you think these four types of attacks should be ranked in terms of exploitation difficulty and severity of harm?

Part Two: Views on MCP Ecosystem Security

1. Have you in the past or would you in the future use AI Agent + MCP methods to manage your private data or resources, such as project source code, personal notes, social media accounts, communication tools, blockchain wallets, online payment platforms, etc.?
2. In your past experience using MCP, did you carefully review the prompt information and permission request information for each execution by MCP applications? Did you pay close attention to their operational details?
3. Regarding MCP server markets/plazas/collection websites like those simulated in the tasks, what role do you think they should play in ensuring user security? What key security indicators or information should they provide?
4. What kind of information, features, or verification mechanisms (such as security scores, user reviews, source authentication, etc.) do you think could significantly enhance your trust in an MCP server?
5. What kind of features and measures (such as sandboxes, gateways, source code audits, etc.) do you expect to improve MCP security risks?

Part Three: Suggestions and Improvements

1. Regarding the overall design of this user research (including the processes of Tasks One, Two, and Three, instructional materials, simulated websites, etc.), do you have any suggestions or think there are areas that could be improved?

Thank you again for investing your time and effort in participating in this user research and interview! Your feedback is crucial for our understanding of users' awareness and needs regarding MCP security.