1) Technical details (approach/technique) that you found novel/ Something specific you learned that you didn't know before

If I didn't get it wrong, the author basically use Function Wrapping in Javascript as well as a series of constraints to make sure that at runtime only authorized external code can access the protected code. In addition, all external code cannot fetch information about the encapsulated code at runtime. What makes this more interesting is that this enhancement is based on purely javascript.

The attack details the authors mentioned in the paper against Facebook are also very interesting as a concrete example of attack against the widely used OAuth 2.0 API. Even the API itself has no problem, inappropriate usage may leave flaws that can be used as exploits.

2)Could I have done this work if I had the idea why or why not?

Logistically speaking I can do the job, because it requires no special resource.

3)Is there anything I could do to repeat or validate?

One thing I can do to validate is the defensive methods mentioned in the paper. I want to validate that by creating a function closure the information of callee will not be disclosed to the caller.

4) What is my best idea for follow on work that I could personally do?

I am personally interested in doing some in-depth research related to javascript. One idea I am currently having in mind is to do the obfuscation / deobfuscation of javascript.

5)What is my best idea for follow on work that I'd like to see the authors do?

I want to see more analysis about how DJS can be used to defend some known type of attacks. In section 6.1, the author mentioned that they have implemented a secret bookmarklet password manager without the need to check window.location. However, they didn't say how they can identify the webpage user is currently viewing without checking the window.location information.

6)Any logistical experimental lessons I learned?

I think I learned nothing related to logistic from this paper.

7)How does this compare to the other papers we read? Most similar? How different? Other comparisons?

This paper addresses several attacking techniques that attack javascript code running in a malicious environment, and suggests a defensive technique based on a series of best practice of coding. This is a new category of attack that is different from the attack techniques we have read before.

8)What is your biggest criticism of the paper?

I have some concern about the security bookmarklet password manager the authors mentioned in the “Application” section. The authors claim that their Defensive Javascript doesn’t allow programmer to access external resource such as “window.location”. However, the bookmarklet password manager’s functionality require it to know the URL of the webpage currently being visited. Without accessing window.location, how could they get this information? The authors didn’t explain this part clearly, nor did they give a substitute to achieve this function. I think this is a problem of this paper.