Reaction to " Eradicating DNS Rebinding with the Extended Same-origin Policy"

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

This paper details Rebind DNS attack, which is what I don't know clearly before. In addition to the attack itslef, the author also details what they have done as a countermeasure to such an attack by proposing a new idea: server-origin to HTTP request. Analysis had been done to different cases of Rebind DNS attack and how their method will work. This is very clear and helpful.

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

If I have the idea, I can do the work without any problem. The work didn't involve any private resource or technique. They mentioned that they modify the source code of Chroium to add their new http header. This part may be a little bit hard, but I believe it will not be a big problem.

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

One thing I can repeat or revalidate is the Rebind DNS attack. According to the description of the attack, I think this attack has a high requirement to the time of modifing DNS entry, which has to be propagated to the victim's DNS after the first request and before the second request. I want to try this attack manually. In addition, I am also interested in the Local Cache API provided by HTML5.

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

I think the author had done a pretty good job about preventing DNS Rebind attack. And this paper arise my interest on other DNS related attack. One thing I can think about is to collect information about all DNS related attack. I want to see whether we can prevent other DNS related attacks by similar methods mentioned in this paper.

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

One thing I want to see the author do is to further investigate other attack related to DNS and see whether they can use similar approach to solve them.

6)Any logistical experimental lessons I learned?

The paper mentioned the open source browser project Chromium, which will be a good testbed if we have ideas of creating new features for browsers.

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

This paper is different frrom the paper we have read before. It talks about an existing type of attack and proposes a way to counter it, which can be categoried as protection. The paper we have read before are mostly about attacking method and exploit that can be used.

8)What is your biggest criticism of the paper?

I have a question about the analysis of how Server-Origin prevent DNS Rebind attack. Basically speaking, the idea of Server-Origin is to let the server itself preserve the identify information, which the author assume the attack should not know and is unique to each server. However, I am thinking that as the author propose to use domain name as server-origin, it would be easy for the attacker to guess the server-origin and use the same value on their faked machine. I would say it will be better to use some meaningless string to prevent this case. Another way will be to use a time-sensitive random value.