Reaction to “Steal This Movie: Automatically Bypassing DRM Protection in Streaming Media Services ”

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

I am not familiar with attack techniques related to reverse engineering before so this paper is definitely a very novel one to me. The paper mentioned a lot of useful tools in reverse engineering like Pin (the dynamic binary instrumentation tool), QEMU (a generic and open source machine emulator and virtualizer) and OllyDbg (32 bit debugger for Microsoft Windows that emphases on binary code). It also mentions many related paper it refers to, which are all very interesting reference for reverse engineering.

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

It is a hard question to answer. Personally speaking, I think reverse engineering is a hard work and even with the idea, I think it would require a lot of knowledge in this area as well as patience to do such a work. At least now, even with the idea, I don’t think I can fulfill the task as the author had done here. However, with some preparation, I can start from some simpler reverse engineering work.

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

The author mentioned the techniques they used in the paper to detect loops in a binary file. One of the paper he refers to (LoopProf: Dynamic Techniques for Loop Detection and Profiling) also talk about this aspect. I can write and compile some sample programs, and use these techniques to verify these techniques.

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

My plan for following work related to this topic is to read through the paper mentioned here as well as other papers related to reverse engineering. Then I will start applying the tricks learnt from these papers to sample applications.

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

I want to see the author talking more about the problems they have encountered in the reverse engineering process. Theoretically I think I can understand what they have done. However there must be more interesting (maybe boring to them) stories when they are doing that. As a beginner of reverse engineering, I think it would be very interesting to read these stories and learn from them.

6) Any logistical experimental lessons I learned?

I don’t think this paper mention about any of this aspect.

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

This is the first paper we have read about reverse engineering, also it is the first paper that I feel like “Oh it’s interesting. However even if I have such an idea it may be hard for me to do the same work.” I have to say that reverse engineering is a brand new area to me and it requires a lot of effort for me to be familiar with this area.

8) What is your biggest criticism of the paper?

One thing I want to criticize about this paper is that although in the paper the author mentioned many methods they used when doing the analysis. The description to these methods are all too brief, without examples from real system to demonstrate problems they have encountered when doing the analysis. Although it could be interpreted as that they want to protect the techniques from being learnt by malicious players, this kind of abbreviation make the paper less convincing.