Software Vulnerabilities: Exploitation and Mitigation

—

Lab 5

Prof. Jacques Klein & Pedro Jesús Ruiz Jiménez
(inspired from Prof. Alexandre Bartel's course)

5 ASLR (40 P.)

First, go through the list of questions. Then, read the paper "Hacking Blind" from Bittau et al. (file: `bittau-brop.pdf`) and answer to the following questions. Please, copy/paste the question in your document before answering it.

Question 5.1 What is BROP? What is the difference between BROP and ROP? (2-3 sentences) — 2 P.

Question 5.2 Does a BROP attack also work for binaries for which the attacker does not have access to (no source, no binary)? Explain. (3-4 sentences) — 3 P.

Question 5.3 Look at Figure 4. Is there a situation where the BROP approach does not work? Why? (3-4 sentences) — 3 P.

Question 5.4 What are the requirements to perform a BROP attack? Explain. (3-4 sentences) — 2 P.

Question 5.5 Instead of randomly brute-forcing the 2^{64} address space, an attacker can leak the return address. How does an attacker leak the return address? Explain. (3-4 sentences) — 3 P.

Question 5.6 What are stop gadgets? What are they useful for? Explain. (3-5 sentences) — 4 P.

Question 5.7 To classify gadgets, different stack layouts (the data the attacker puts on the stack) are used? What are the different stack layouts and how can they be used to identify categories of gadgets? Explain. (5-10 sentences + figure) 5 P.

Question 5.8 To execute a function, the attacker has to find the PLT. What is the PLT? How can an attacker find this table? Explain. (5-10 sentences + figure) 5 P.

Question 5.9 How long, did it take to exploit a vulnerability with a BROP attack in yaSSL + MySQL? in nginx? 3 P.

Question 5.10 The return address might not be recovered if a load balancer is used (we assume here attack on a remote host through the network). Explain why. (5-10 sentences + figure) 5 P.

Question 5.11 The attack might not work if all workers are stuck in a loop. Explain why. (5-10 sentences + figure) 5 P.

Note on plagiarism

Plagiarism is the misrepresentation of the work of another as your own. It is a serious infraction. Instances of plagiarism or any other cheating will at the very least result in failure of this course. To avoid plagiarism, always cite the source from which you obtained the text.