Veton Abazovic

NetID: va187

Computer Security

3/6/2019

Assignment 5

Question 1

(a) What does the match for pattern1 test?

Answer: The match for pattern1 test the code in the UNIX “login” command.

(b) What does “bug 1” do?

Answer: The bug1 allows a user with a known password to login as any user.

(c) What is the purpose of the second pattern match in the C compiler - the one that inserts “bug 2”?

Answer: The second pattern match in the C compiler would insert both trojan horses in the compiler.

(d) What does “bug 2” accomplish?

Answer: Bug 2 will self-replicate into the C binary that will reinsert the bug into the compiler.

Question 2

What does David A. Wheeler propose as a test to determine if a compiler has been made untrustworthy?

Answer: David A. Wheeler purposed that to deem a compiler trustworthy or not we would have to compile the code twice, one time being compiled on a trusted compiler and then another time on the compiler in question. Then we compare the results bit by bit and if they match we can then determine the compiler is trustworthy. If the bits are not the same the compiler is not deemed trustworthy.

Question 3

(a) How would an NaCl container, which is forbidden from accessing a system’s storage, be able to offer store and retrieve local files if needed?

Answer: NaCl container is able to offer store and retrieve local files if needed by a service runtime interface which allows access to systems calls. It passes information from the channel to NaCl and then opens an imc channel to the storage device.

(b) The inner sandbox allows us to place a trusted service runtime subsystem within the same process as the untrusted application module. What two mechanisms are used by the inner sandbox subsystem to keep applications from doing harm?

Answer: There are two mechanisms that are used by the inner sandbox subsystem to keep applications from doing harm. One being that the inner sandbox uses static analysis to detect defects in untrusted machine instructions. The other being that the inner sandbox uses segmented memory to constrain data and instruction memory references.