ENPM809W – Introduction to Secure Coding

Homework – 5

Author – Syed Mohammad Ibrahim

UMD ID: iamibi

Email: iamibi@umd.edu

1. The paper suggests that CSRF vulnerabilities still abound despite the protection mechanisms that are currently available. True or False.

A. True

2. The paper references Code Property Graphs or CPGs, which assume that transfer of control only happens via function calls. However, in Javascript, transfer of control also happen via events from the environment (for example, mouse-events or user-defined events. The paper references Listing 1 here. Which line(s) of Listing 1 shows this?

A. Line number 3, 4 and 5.

3. As per the paper, a Code Property Graph is a combination of which three representations of the C source code?

A. A Code Property Graph is a combination of the following three representations of the C source code:

- Abstract Syntax Tree
- Control Flow Graph
- Program Dependence Graph

4. What is the paper trying to do with the PDG, CFG, IPCG, and ERDDG for detecting client CSRF?

A. To detect the client-side CSRF, the authors want to identify the statements that send HTTP requests and those which consume data values from pre-defined sources. They want to model the properties of statements via semantic type. An example mentioned in the paper, the authors want to assign the type WIN.LOC to window.location and propagate it through PDG, CFG, IPCG and ERDDG edges.

5. How do the authors handle third party libraries for doing what is being done in Question 4 above?

A. The authors extract the symbolic model for each library and use it as a proxy for the analysis of the application code. The symbolic model in this context is an assignment of symantic types to libraries' functions and object properties.

6. What inputs does JAW take for performing the client side CSRF analysis?

A. JAW takes a seed URL of a website as an input, visits the website using a JavaScript enabled web crawler to collect the web resources. On the way, it also collects run time state values.

7. The JAW analysis also reports False Positives (where JAW says there is a potential CSRF possible, but it is not). True or False.

A. True

8. The authors of JAW identified 9 applications that allow an attacker to modify the URL domain making it possible to do cross-origin requests. Are the authors assuming that CORS is enabled for the web application? Yes or No? Why?

A. Yes, the authors are in assumption that the CORS is enabled since they are performing a cross-origin attack.

9. The authors point out that the client-side CSRF attacks also enable other kinds of attacks. What are those attacks?

A. The other attacks that can be mounted are XSS and SQLi.

10. As per the authors, how many percentage of application was the attacker able to overwrite a parameter in the request body to perform the client-side request forgery?

A. 28.7%