IN5100: Uncovering Security Flaws in Browsers using Maude

Peter Ölveczky

October 18, 2023

As always, try to understand the main concepts. In particular, no (non-trivial) background in web browser implementation is assumed.

Curriculum (pensum)

The curriculum is defined by the (entire) paper

> Shuo Chen, José Meseguer, Ralf Sasse, Helen J. Wang, and Yi-Min Wang:
>
> *A Systematic Approach to Uncover Security Flaws in GUI Logic.* In: Proc. IEEE Symposium on Security and Privacy 2007.

and the lecture presenting this stuff. This paper should be available through UiO at `https://doi.org/10.1109/SP.2007.6` (I can email it to you if you cannot get access to it.)

Some Things to Think About

- What are the main two things that can go wrong? That is, what kinds of flaws are the authors searching for?
- For status bar attacks, what kind of web pages are the authors analyzing? Why do they claim that this is "sufficient"?
- What is roughly the authors' methodology?
- What do the authors do when their formal analysis discovers a (possible?) attack?
- What do we need to include in the "modeled state" in addition to the "state of the browser"?
- How do the authors represent the "structure of a web page"?
- Note that no detailed knowledge about how a browser handles events is needed, just a rough intuition about what's happening.
- For the two categories of errors the authors are analyzing (in Sections 3 and 4, respectively), what particular "features"/"events"/"behaviors" of web browsing are they modeling?
- To analyze status bar spoof attacks, what is the authors' main approach?

  - what is the main property that should be satisfied?

- In Section 3, what are the challenges/difficulties of analyzing exhaustively for all user actions and all (HTML) web pages? How is this "solved/addressed/approached" in the paper? What are the restrictions?
- What happens in the rules on the middle of page 7 of the paper? And what happens in the search command on page 7?
- Give some intuition about the kinds/causes of the errors in browsers found in Section 3.
- In the analysis in Section 4, why cannot we be sure that attacks/security flaws found by Maude analysis are *real* attacks?
- How is the analysis performed in Section 4?
- Can you give a *high-level intuition* about the different "kinds/causes" of flaws found in Section 4?
- What do the authors claim are disadvantages/advantages with Maude analysis vs. testing using *Detours*?