Workshop in compile-time techniques for detecting Javascript exploits

Shir Landau-Feibish, Shmulik Regev, Noam Rinetzky

http://www.cs.tau.ac.il/~maon/teaching/2013-2014/workshop/workshop1314b.html

Semester B. Monday, 16:00-18:00. Kaplun 319

Scope

- Automatic tools for analyzing Javascripts
- Detecting malicious code

- Static tools: Compile-time
- Dynamic tools: Run-time

Admin

- Projects in groups of 2-3
- Talking and helping is OK
  - Copying is not
- All members should participate
- Hands-off guidance

Goals

- Learn Javascript
- Implement a simple analyzer (mini-project)
- Implement a sophisticated analyzer
  - Choose a vulnerability
  - Find tell-tale signs
  - **Implement a detector**
    - Compile-time analysis
    - Can have a runtime component
- Experimental evaluation
- Presentation of tools & results

Short term schedule

- Today: Problem description

- Next week:
  - Review of existing tools/techniques
  - Mini-project description

Long Term Schedule

(Tentative)

- 17/02/2014: Problem description
- 24/02/2014: Mini-project description
- 07/04/2014: Progress report (mini project)
- 09/06/2014: Progress report
  - Mini project submission
  - Presenting chosen project
- 02/09/2014: Project submission
- ~15/September/2014: Project presentation

Javascript

- Self study

- Next lecture in Programming Languages
  - Next Monday (24/2/14), 10:00-12:00
  - Dan David 001

Next week: Review of Techniques&Tools

- Heap feng shui
- Address disclosure
  - Pointer inference + integer sieve sections
- JIT spray
  - JIT spry Section
- ROP
  - Sections 1-2
- Zozzle

Text links

- Heap feng shui
  - https://www.usenix.org/legacy/events/woot08/tech/full_papers/daniel/daniel_html/woot08.html
- Address disclosure
  - http://www.semantiscope.com/research/BHDC2010/BHDC-2010-Paper.pdf
  - Pointer inference + integer sieve sections
- JIT spray
  - http://www.semantiscope.com/research/BHDC2010/BHDC-2010-Paper.pdf
  - JIT spray section
- ROP
  - http://cseweb.ucsd.edu/~hovav/dist/geometry.pdf
  - Only sections 1 & 2
- Zozzle
  - http://research.microsoft.com/apps/pubs/?id=141930